WWW.HACKERJOURNAL.IT

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

N° 205

DIRECTORY

SICUREZZA
>KERBEROS A GUARDIA DELLA RETE

INTERNET
>PLONE & RSS
>POSTA CON PHP

SICUREZZA
>GLI EXPLOIT DEL MESE

IN PRIMO PIANO



NAGIOS

ALLA SCOPERTA DI UN OTTIMO STRUMENTO OPEN SOURCE DI MONITORAGGIO DEI SERVIZI DI UNA INTRANET

SECURITY LAB

IL NUOVO INSERTO DEDICATO ALLA SICUREZZA

COMPUTER
MAC E UNIX: I COMANDI

SINTASSI
ESPRESSIONI REGOLARI CON REGEX COACH

HACKER JOURNAL N° 205 - MENS - ANNO 10 - € 2,00

WLF PUBLISHING

00205

9 771594 577001

LAVORI IN CORSO

È passato un mese dall'annuncio del cambio di periodicità di HJ e in questo numero 205 si cominciano ad intravedere alcune delle modifiche che avevamo in parte annunciato sul numero 204. In primo luogo una grafica più sobria, poi una specie di sezione speciale, Security Lab, che fa parte di un percorso particolare che abbiamo voluto intraprendere per capire se ci può essere spazio per una rivista parallela ad HJ, ma rivolta soprattutto alla sicurezza e trattata in chiave decisamente professionale (non che HJ, non lo sia, ma vorremmo capire se tra i numerosi professionisti IT che ci seguono ci possa essere questo genere di aspettativa). Vedremo…

Ma torniamo al presente, ovvero ad HJ. Al di là di tutte le modifiche che abbiamo apportato e apporteremo, la notizia più importante è l'affetto manifestato dai lettori e il loro incoraggiamento giunto sia via mail che attraverso le pagine del forum.

La comunità di Hacker Journal è ricca di spunti, appassionata e tenacemente attaccata a queste 32 pagine aperte sul mondo underground. Per quanto ci riguarda vogliamo ripartire proprio da qui con tanto entusiasmo e l'apporto di tutti.

Nel frattempo stiamo anche lavorando alla versione pdf da distribuire attraverso l'abbonamento on-line. Evidentemente questo comporterà una serie di modifiche tecniche all'infrastruttura del sito e ci vorrà qualche tempo, ma vi terremo informati… non temete.

… e come sempre: buona lettura

Altair

laboratorio@hackerjournal.it
Questo indirizzo è stato creato per inviare articoli, codici, spunti e idee. E' quindi proprio una sorta di "incubatore di idee".

posta@hackerjournal.it
E' l'account creato per l'omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.

redazione@hackerjournal.it
Questo è l'indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.

Sommario

Anno 10 - N.205
Settembre 2010

Editore (sede legale)
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71 - 00196 Roma
Fax 063214606

Realizzazione editoriale
Progetti e promozioni Srl
redazione@progettiepromozioni.com

Printing
Grafiche Mazzucchelli S.p.a - Seriate (BG)

Distributore
M-DIS Distributore SPA
Via Cazzaniga 19 - 20132 Milano

Hacker Journal
Pubblicazione registrata
al Tribunale di Milano il 27/10/03
con il numero 601.
Una copia: 2,00 euro

Direttore Responsabile
Teresa Carsaniga
redazione@hackerjournal.it

Direttore Editoriale
Andrea Franchini



Internet
SEMPRE PIÙ VELOCE

È stato pubblicato di recente un rapporto, da Akamai, sullo stato di internet che tocca diversi argomenti: l'origine degli attacchi informatici, l'adozione di banda larga e la connettività mobile, tra gli altri. Il dato riguarda un campione di oltre 70.000 server che gestiscono il 20% del traffico online globale. La città più veloce, in termini di scorribande via internet è, forse un po' a sorpresa ma non troppo: Masan (Corea del Sud). Con 59 città su 100, il Giappone ha il primato del maggior numero di città con la connessione più veloce, mentre sono solo 12 le città degli Stati Uniti incluse nella classifica. Umea in Svezia, è la più veloce tra le 11 città europee presenti nell'elenco e si è classificata al 18° posto. Interessanti anche i dati sulle velocità massime di connessione. L'Asia è in testa anche in questa classifica, con Corea del Sud, Hong Kong e Giappone ai primi tre posti fra i 10 Paesi più veloci. Prima in assoluto è la Corea del Sud, con una media di 33 Mbps di velocità massima. In Italia, la media delle velocità massime di connessione è di 10,2 Mbps. Per quanto riguarda l'Europa, Romania, Svezia, Lettonia, Belgio, Portogallo e Bulgaria occupano 6 dei rimanenti 7 posti in classifica, tutti registrando velocità massime di connessione in media superiori ai 15 Mbps, mentre gli Stati Uniti si sono piazzati ottavi con 16 Mbps.Nei dieci Paesi con la maggiore velocità di connessione media l'aumento di velocità è stato contenuto, con Hong Kong e Danimarca rimaste sostanzialmente stabili, mentre Giappone, Olanda e Svizzera hanno migliorato la velocità media del 3,5% circa rispetto allo scorso trimestre. In Italia, la velocità media di connessione è di 2,85 Mbps.

CONNETTIVITÀ INTERNET

Nel primo trimestre del 2010, oltre 487 milioni di indirizzi IP unici si sono collegati da 233 Paesi alla rete di Akamai, con un aumento del 7,2% rispetto al quarto trimestre 2009 e del 16% rispetto allo stesso trimestre dell'anno precedente. Mentre la variazione su base annuale è abbastanza coerente con i livelli osservati nell'ultimo trimestre del 2009, i cambiamenti su base trimestrale hanno registrato una crescita di circa il 75% rispetto al trimestre precedente, dato che indica un aumento del livello di penetrazione di Internet.Stati Uniti e Cina continuano a rappresentare circa il 40% degli indirizzi IP monitorati. Sono stati individuati 184 Paesi con meno di un milione di indirizzi IP unici connessi alla rete di Akamai nel primo trimestre del 2010. In termini di crescita annuale del numero di indirizzi IP unici monitorati da Akamai, la Cina ha registrato un aumento del 30%, più del doppio della crescita osservata negli Stati Uniti.

CONNETTIVITÀ MOBILE

Come nel quarto trimestre del 2009, continua in Italia il divario di circa 2 Mbps tra il provider che offre la maggiore velocità media di connessione mobile (2,72 Mbps) e quello che offre la velocità minore (0,85 Mbps). Le velocità di connessione mobili più alte registrate in Italia vanno, a seconda dell'operatore, dai 4,73 Mbps ai 9.66 Mbps. La media delle velocità massime registrate nelle reti mobili in tutto il mondo sono state piuttosto alte, con 83 operatori su 109 che hanno superato la soglia dei 2 Mbps di velocità; 33 hanno registrato valori superiori ai 5 Mbps e 6 hanno addirittura oltrepassato i 10 Mbps.

ATTACCHI INFORMATICI

Nel primo trimestre del 2010 sono stati registrati attacchi informatici provenienti da 198 Paesi. In testa ancora la Russia, per il terzo trimestre consecutivo, con il 12% del totale degli attacchi. Al secondo e al terzo posto si collocano gli Stati Uniti (10%) e la Cina (9,1%), seguiti da Taiwan e Brasile. Come nel quarto trimestre del 2009, l'Italia si posiziona al sesto posto, con il 4,4% del totale degli attacchi.

ATTENZIONE LA SESTA PARTE DEL CORSO IN C, PREVISTA PER QUESTO NUMERO 205, SARÀ PUBBLICATA SUL PROSSIMO NUMERO, IL 206.

Arriva in Polonia il primo bancomat biometrico



Sarà la Polonia il primo stato europeo ad installare presso le banche BPS il bancomat biometrico.
Si tratta di un'innovazione basata sulla tecnologia sviluppata dalla società giapponese Hitachi e largamente in uso in Giappone.
La novità consiste nel fatto che non ci si dovrà più ricordare il tanto odiato PIN per poter effettuare un'operazione al bancomat ma sarà sufficiente appoggiare il proprio dito sull'apposito lettore. A questo punto l'identificazione non avverrà tramite lettura delle impronte digitali bensì verrà riconosciuto lo schema delle vene delle dita che verrà confrontato con l'immagine in possesso della banca.
"Si tratta di una tecnica maggiormente affidabile rispetto a quella del riconoscimento delle impronte digitali," afferma Peter Jones, responsabile della sicurezza di Hitachi Europa.
"A differenza delle impronte digitali, che lasciano una traccia e che possono essere potenzialmente riprodotte, le vene delle dita sono impossibili da replicare, perché si trovano sotto la superficie della pelle" continua Jones.
Il primo bancomat biometrico in Polonia è già stato installato in una delle filiali della banca BPS di Varsavia ed entro la fine dell'anno ne dovrebbero essere installati altri quattro.
Il bancomat biometrico è molto diffuso in Giappone dove le banche, in seguito ad una legge del 2006 rispondono delle truffe e dei furti subiti dai loro clienti.
Ad oggi in Giappone si contano 80.000 bancomat biometrici ma ce ne sono altri installati in altre parti del mondo quali Asia, America Latina e qualcuno persino in Africa.
In Europa questa nuova tecnologia non è ancora in uso per diversi motivi: primo tra tutti, lo scarso interesse da parte delle banche, che per installare bancomat di questo genere dovrebbero spendere parecchio denaro senza avere in cambio nessun vantaggio (attualmente in Europa se vengono compiute frodi o viene rubato denaro agli utenti sono questi che vengono penalizzati, la banca non ne è responsabile).
La Polonia al contrario è molto attenta alle nuove tecnologie, settore in crescita nel paese e in cui il Governo ha deciso di investire molto, facendo di questo il fulcro su cui incentrare la crescita economica dei prossimi anni.





YOU TUBE BUCATO

Si dice sempre di chi viene bene in video che buca lo schermo, logico, per la legge del contrappasso, che proprio un sito di video abbia subito la sorte di essere stato "bucato". E' accaduto il 4 Luglio, la festa dell'indipendenza in America, al popolare YouTube. Si è trattato di una attacco XSS più familiarmente noto come Cross Site Scripting. Poche righe di codice inserite nei commenti dei filmati del cantante Justin Bieber che dirottavano gli utenti ad un sito hard a pagamento. La tecnica XSS sfrutta in realtà una vulnerabilità dei siti dinamici e consente di carpire informazioni sostanzialmente in due modi: attraverso il browser dell'utente che si connette alla pagina web modificata (a sua insaputa) e accedendo ai suoi cookie, ovvero i micro frammenti di software che vengono installati nel Pc dell'utente quando visita un sito e che consentono, al sito stesso, di riconoscerlo in automatico ai collegamenti successivi. Oppure indirizzando l'utente su una pagina web fraudolenta con lo scopo di fargli inserire, e quindi rubare, dei dati sensibili.
Probabile che la vulnerabilità di YouTube sia stata scoperta mandando in esecuzione un semplice javascript. Gli amministratori di sistema hanno comunque informato che il problema è stato risolto e, per il momento aggiungiamo noi, YouTube è tornato ad essere sicuro.

YouTube™

APPLE STORE SOTTO ATTACCO

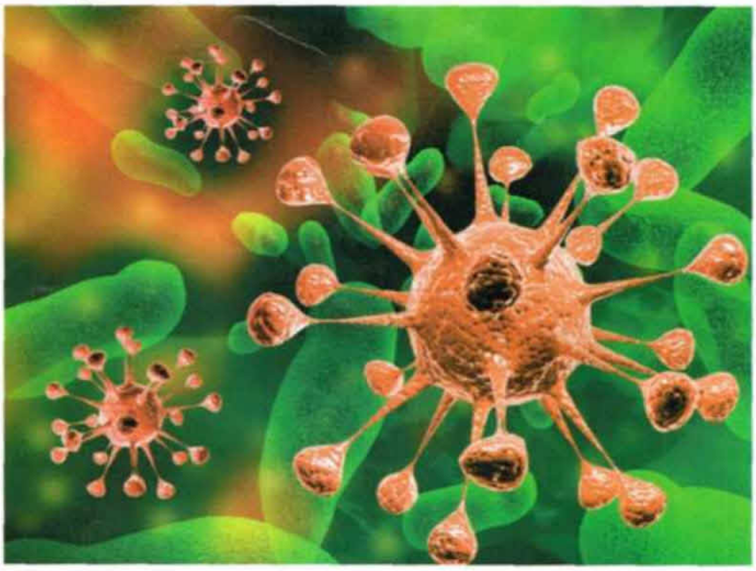


Il noto Store di Apple ha subito un attacco senza precedenti. Numerose sono state le segnalazioni di utenti i cui account di iTunes sarebbero stati violati da hacker che si sarebbero appropriati di password e informazioni riservate relative a carte di credito e successivamente utilizzate per effettuare acquisti di applicazioni non autorizzati. L'attacco è partito negli Stati Uniti dove gli account interessati sono stati veramente molti per poi diffondersi in Europa, sono pervenute segnalazioni dall'Inghilterra. Le prime notizie su ciò che stava accadendo sono stati dei messaggi diffusi su Twitter. La Apple non ha ancora rilasciato nessun commento ufficiale e l'unica soluzione praticabile per risolvere il problema al momento sembra essere quella del cambio di password.



Nuova tecnologia ANTI-MALWARE

Oggi il malware ha la capacità di diffondersi a macchia d'olio, un'epidemia diffusa via Internet può infettare milioni di computer in un solo istante. Queste epidemie possono pregiudicare molte infrastrutture informatiche, portando al collasso le autostrade dell'informazione, creando vulnerabilità nei sistemi con relative perdite di dati e la diffusione di frodi informatiche su larga scala.
Il rilevamento di malware su tutti i computer che sono stati infettati durante una epidemia ha poco o nessun effetto. Ciò che occorre è un metodo affidabile per valutare le dimensioni potenziali e l'evoluzione di una epidemia, un sistema di allarme preventivo, e questo è esattamente ciò che la nuova tecnologia sviluppata da Yury Namestnikov, Nikolay Denishchenko e Pavel Zelensky di Kaspersky Lab è in grado di fare. La tecnologia ha ottenuto il brevetto Nr. 7743419 del US Patent and Trademark Office il 22 giugno 2010.
La nuova tecnologia brevettata permette di analizzare le informazioni statistiche sulle minacce ricevute da una rete di monitoraggio globale. La rete analizza i download di malware, gli attacchi hacker e altre simili minacce di sicurezza, registrando i tempi in cui si verificano, la loro origine e la posizione geografica ecc.. Le epidemie emergenti possono quindi essere identificate dal numero di incidenti che si verificano nel corso di un determinato periodo o in un determinato luogo. Questo metodo rende facile individuare l'origine di un'epidemia e prevedere il suo probabile modello di propagazione.
Le misure di protezione possono essere sviluppate e implementate dai paesi interessati dall'epidemia, rallentando così considerevolmente il tasso di proliferazione, fornendo un'efficace limitazione dei danni. Il monitoraggio, la rilevazione e l'analisi dei dati viene effettuata in tempo reale, rendendo questa tecnologia brevettata particolarmente efficace contro le epidemie di malware che si diffondono rapidamente.
"Il nuovo sistema offre molti vantaggi rispetto a soluzioni analoghe. Questa tecnologia contiene un sottosistema capace di rintracciare la fonte della minaccia, un modulo che genera misure di protezione e un sottosistema che simula la diffusione dell'epidemia", sottolinea Nadia Kashchenko, Chief Intellectual Property Counsel di Kaspersky Lab.
Ad oggi Kaspersky Lab ha depositato più di 50 domande di brevetto negli Stati Uniti, Russia, Cina ed Europa: tecnologie di sicurezza ideate e sviluppate dai tecnici dei Laboratori Kaspersky.



Arriva il pulsante antipanico

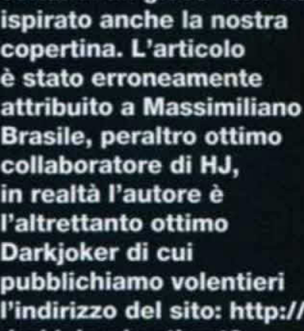
Per la sicurezza degli utenti più giovani di Facebook è stato introdotto il "pulsante antipanico". Il noto social network ha accettato di inserire nelle proprie pagine la nuova applicazione che consentirà di segnalare comportamenti, o contenuti ritenuti scorretti direttamente all'agenzia governativa britannica che si occupa della protezione e del controllo dei minori su internet: la Child Exploitation and Online Protection Centre (Ceop).
Finalmente, gli adolescenti saranno più tutelati, sarà sufficiente installare l'applicazione direttamente sul proprio profilo per potervi accedere. Dopo mesi di discussione, Facebook era dapprima recalcitrante, si è giunti a questa decisione anche grazie alla condanna all'ergastolo di Peter Chapman accusato di aver stuprato ed ucciso una studentessa diciassettenne conosciuta proprio su Facebook, che ha interessato l'opinione pubblica nei giorni scorsi. Il primo social network ad installare il "panic button" è stato MySpace lo scorso novembre.
I siti web di social networking sono un fenomeno culturale recente. Facebook ha attualmente più di 300 milioni di utenti attivi, 150 milioni dei quali si collegano almeno una volta al giorno. Ogni utente ha in media 130 'amici', ma molte persone, soprattutto i giovani, non prestano attenzione alle impostazioni di sicurezza, dando così la possibilità a tutti di leggere le loro informazioni riservate, esponendosi così a grossi rischi.

PayPal il più colpito

PayPal rimane l'obiettivo principale dei criminali informatici: a giugno, il numero di attacchi rivolti a questo sistema di pagamento elettronico è aumentato di 20 punti percentuali rispetto a maggio.
Tre paesi - Brasile, Colombia e Spagna - risultano tra i primi 5 distributori di spam. Una nuova tendenza ha inoltre interessato il malware contenuto nel traffico e-mail - il numero di programmi maligni che lavorano su piattaforma Win32 è in calo, mentre al contrario, la quota di HTML risulta in crescita. La maggior parte dei programmi maligni nel mese di giugno inclusi nella Top 10, sono pagine HTML scritte in JavaScript. Ciò ha fatto sì che molti utenti fossero reindirizzati a siti web contenenti spam, oltre ad una serie di diversi exploit. Date queste premesse è ragionevole pensare che la distribuzione di massa di questo tipo di e-mail continuerà nei prossimi mesi. Le varianti di uno dei rootkit più pericolosi attualmente in circolazione, Trojan.Win32. TDSS, sono state distribuite anche via e-mail nel mese di giugno, due di loro hanno raggiunto il quarto e settimo posto nella Top 10. Le varianti di questo programma potrebbero essere trovate in diversi link, anche se sempre sotto forma di un allegato compresso in un archivio zippato. Per diffonderli, i truffatori utilizzano uno dei loro temi preferiti - le tasse.

Rettifica articolo
"Bypassare la richiesta di serial di un gioco"

Diamo a Cesare quello che è di Cesare. Nel numero 204 abbiamo pubblicato un ottimo articolo intitolato "Bypassare la richiesta di serial di un gioco" che ha ispirato anche la nostra copertina. L'articolo è stato erroneamente attribuito a Massimiliano Brasile, peraltro ottimo collaboratore di HJ, in realtà l'autore è l'altrettanto ottimo Darkjoker di cui pubblichiamo volentieri l'indirizzo del sito: http:// darkjoker.byethost9.com.



Massimiliano Brasile
redazione@hackerjournal.it

RegEx Coach

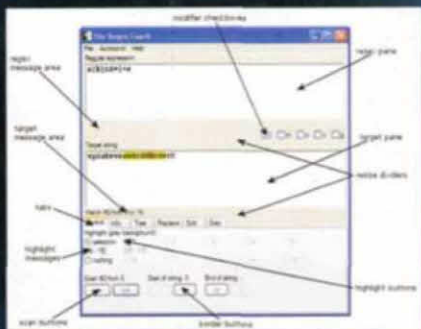


Ci piace smanettare e grazie al web abbiamo allargato i nostri orizzonti avendo a disposizione enormi quantità di dati e informazioni sulle quali fare scraping a nostro piacimento, o perché vogliamo scrivere un nostro webbot che faccia concorrenza ai google-bot o semplicemente perché amiamo ottimizzare il tempo e far fare il lavoro sporco ai nostri droni.
Non possiamo quindi non conoscere le regular expression (per gli amici RegEx), ma a meno di averle mangiate e metabolizzate da anni, avremo sempre bisogno di una guida di riferimento e anche qualche esempio applicativo per ottenere al volo il dato che stiamo cercando in mezzo a quel mare di dati.
Il Dr. Edmund Weitz, uno sviluppatore free-lance tedesco, ha però realizzato un tool freeware chiamato RegEx Coach (googla e lo trovi come primo risultato) che permette di risparmiare molto tempo dato che effettua il parsing in tempo reale della regular expression che inseriamo dandoci subito il risultato sui dati che gli passiamo da analizzare.

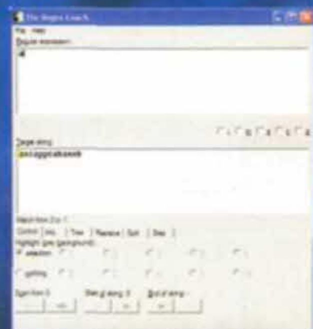
SINTASSI
LA PALESTRA PER LE ESPRESSIONI REGOLARI SEMPRE PRONTA!

CARATTERISTICHE

Una premessa dovuta: in base al linguaggio di programmazione che utilizziamo, l'implementazione delle RegEx potrebbe essere o meno efficiente e completamente compliant con quella del Perl. RegEx Coach si rivolge soprattutto ai programmatori perl e quindi la notazione usata sarà quella.
Se questa limitazione non è un problema, installiamo l'eseguibile di RegEx Coach e siamo pronti per le prove.
L'interfaccia è minimale con una classica struttura a due box: uno per l'inserimento (Regular expression) e uno per l'output (Target string). E' possibile scrivere anche nella finestra di output, dal momento che possiamo inserire direttamente il testo sul quale eseguire i nostri test e non appena digitiamo qualcosa nella finestra di input saranno evidenziati in rosso gli errori di sintassi, in giallo le corrispondenze (match) identificate



Interfaccia semplice ma efficace direttamente utilizzabile per scrivere e testare le espressioni regolari.

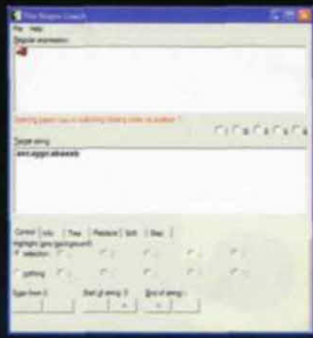


Appena iniziamo a scrivere un'espressione regolare, viene direttamente eseguita sulla Target string evidenziando in giallo i match.

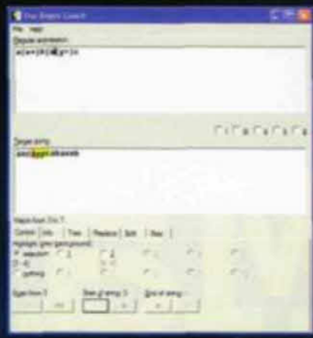
in base alla regular expression che abbiamo composto.
Già con questa funzionalità di base, RegEx Coach permette di risparmiare molto tempo valutando in tutta calma l'analisi che stiamo ricercando. Torna però utile anche per verificarne la ricorsività, tramite le frecce di Scan in basso, nel caso le corrispondenze siano più di una. E' possibile poi "nascondere" al tool i primi caratteri di quanto inserito nella Target string, magari perché stiamo rifinendo proprio una ricerca interna. Se poi, con la ricerca svolta andiamo a selezionare parte della regular expression, sarà eseguita tale sotto-regular expression sul risultato attualmente evidenziato in giallo, con una sottolineatura in arancione e viene indicata anche la posizione del "match".
Nel caso però che la sotto-espressione non sia valida, la sottolineatura arancione non comparirà e il radio-button selection verrà disabilitato.

PANNELLI

Oltre al pannellino di controllo, sono disponibili altri interessanti fogli. In Info viene "interpretata" a parole la regular expression inserita, chiaramente in modo molto semplificato.
In Tree possiamo vedere la nostra espressione regolare esplosa come rami di un albero: in pratica possiamo vedere come RegEx Coach effettua il parsing dell'espressione che abbiamo inserito.
Replace invece, come suggerisce il nome, ci permette di elaborare l'espressione regolare in grado di effettuare sostituzioni all'interno della stringa Target, con un meccanismo apparentemente poco immediato: nella finestra Target selezioniamo con il mouse la parte di stringa che vogliamo sostituire, mentre nel campo Replacement string del foglio Replace inseriamo il carattere sostitutivo. Otterremo in Replacement result il risultato atteso in cui la parte selezionata viene sostituita con la stringa in Replacement string.



Se l'espressione inserita non è valida, nella finestra di inserimento saranno sottolineati in rosso i caratteri in errore.

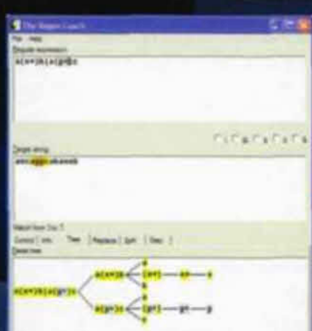


Selezionando parte dell'espressione regolare, sarà evidenziata in arancione la sotto-ricerca richiesta.

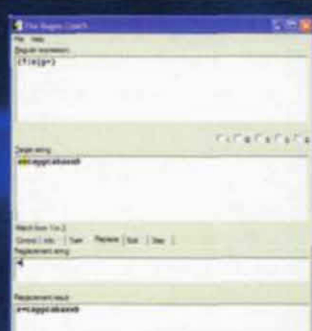
Se selezioniamo il modificatore g (globale) vedremo tale sostituzione applicata su tutta la stringa Target e non solo sulla prima occorrenza. Gli altri modificatori, mutuati sempre dal Perl, permettono di discriminare diversi parametri:
i, case-sensitive e case-insensitive m, per gestire più righe come se fosse una sola s, per rilevare o meno il carattere di nuova riga (new line) x, aumenta la leggibilità del pattern potendo inserire spazi bianchi e commenti.
Split funziona in modo simile a Replace, con la differenza sostanziale che invece di sostituire la stringa selezionata, utilizza la stringa inserita in Split string come delimitatore per spezzare la stringa Target. E' possibile clonare il comportamento di Split del Perl utilizzando la casella Limit: questo parametro (se inserito) indica in quante parti al massimo dividere la stringa. In Divider possiamo selezionare il simbolo grafico da utilizzare per visualizzare le parti della stringa divisa.
In Step infine è possibile percorrere tutti i passi compiuti da RegEx Coach per eseguire l'espressione regolare inserita e valutare la correttezza dei risultati parziali, oltre di quello finale.

CONCLUSIONI

**RegEx Coach può essere visto sia come un coltellino svizzero per le espressioni regolari, che come un'utilissima palestra che possiamo usare per verificare al volo un pattern o per esercitarci costantemente in questo linguaggio utile in molti campi.
Il programma è gratuito e occupa davvero poco spazio e, personalmente, ha trovato subito posto nella mia fedele penna usb ;)
Consigliatissimo!**



Tree visualizza graficamente la nostra espressione regolare lasciandoci comprendere come il tool la sta analizzando.



Per testare le sostituzioni andiamo in Replace e inseriamo il testo da sostituire; poi selezioniamo nella Target string la parte che vogliamo modificare.

di Massimiliano Rinaldi
redazione@hackerjournal.it

Mac in Unix X

SYSTEM

MINI GUIDA ALL'UNIVERSO COMPOSITO DEI COMANDI UNIX SU PIATTAFORMA MAC.

Gli utenti Mac con il passaggio al system X *hanno iniziato ad* apprezzare la solida architettura Unix su cui sono imperniati Leopard e Snow Leopard (ma anche Panther, Tiger e gli altri system ispirati ai felini). In questo brevissimo articolo vedremo di conoscere ed apprezzare i principali comandi Unix.

Unix ha centinaia di comandi standard. La sua filosofia è di avere tanti piccoli comandi ognuno dei quali ideato per fare esattamente una cosa: quella giusta. Ad esempio, un'applicazione Macintosh può essere chiamata Super File Amico. La nostra applicazione immaginaria può fare qualsiasi cosa con qualsiasi tipo di file (una specie di genio della lampada in ambito informatico): può mostrare il contenuto di un file, duplicare un file, rinominare un file, cancellare un file, e persino leggere un file. In Unix, tutte queste funzioni sono possibili attraverso l'uso di programmi distinti: cp, mv, rm, e cat. Tutti questi piccoli comandi possono essere combinati per realizzare qualsiasi risultato desiderato, perché la piccola dotazione di programmi specializzati fornisce un incredibile livello di flessibilità.

LA SINTASSI DEI COMANDI UNIX

La forma base di un comando Unix è

```
command-name options arguments
```

Il command-name è il nome del comando Unix, come ad esempio ls o mv. Options (chiamate anche Switches o Flag) sono le opzioni che è possibile specificare per modificare il comportamento predefinito del comando e di solito sono precedute da un segno meno (-). Arguments sono stringhe (spesso, ma non sempre, i nomi dei file) che forniscono il comando di ingresso e possono anche specificare la destinazione di uscita. Il comando per cancellare la directory chiamata "MyFolder", ad esempio potrebbe leggersi:

```
rm -R myfolder
```

dove "rm" è il comando (commamd-name) di soppressione del file, "-R" è l'opzione (option) che specifica la ricorsione (trasver-

sale e, nel caso del comando rm, la rimozione di file e gerarchia di directory all'interno della directory specificata), e "MyFolder" è l'argomento (argument), e in questo caso, anche il nome del file.
I comandi Unix sono la CLI equivalente delle applicazioni Mac OS X, e del menu di selezione. Anche se i file di comando Unix possono essere posizionati in qualsiasi punto del file system in cui si ha il permesso di accesso, tradizionalmente, si trovano in una delle directory più consuete come / bin, / usr / bin, / sbin, o / usr / sbin. Altre directory sono specificate dalla variabile di ambiente PATH. (Ad esempio occorre digitare echo $ PATH nel Terminale per cercare automaticamente le directory, separate da due punti, che contengono i comandi.) Se il comando non si trova in una di queste directory, la sua ubicazione, deve essere pienamente specificata per la shell al fine di eseguire il comando. È possibile navigare in queste directory attraverso il Terminale utilizzando il comando ls. Si può provare a digitare ls / bin per visualizzare i file di comando elencati nella directory / bin. In questo esempio, "ls" (elenco di directory contenuti) è il comando. Non ci sono options in questo caso, e la "/ bin" è l'argomento (argument), che rappresenta ancora una volta il nome di un file (nello specifico, una directory).

Un tradizionale file system Unix distingue tra maiuscole e minuscole nella denominazione di file e directory, quindi il file chiamato INSTALL e diverso dal file denominato install, che a sua volta è diverso dal file chiamato Install. Mac OS risolve il problema facendo in modo che i nomi di file non siano case-sensitive nella GUI, ma caso per caso, la sensibilità è ancora la regola quando si sta lavorando nella shell.



MAN PAGE

Una delle cose migliori della maggior parte dei componenti di Unix è la loro provenienza, con una documentazione completa, costruita su misura per il sistema. Mac OS X è un ottimo esempio di questa logica. La documentazione Unix è disponibile sotto forma di pagine di manuale, meglio conosciute come man page. In Unix, ogni programma ha un corrispondente man page. Se c'è il bisogno concreto di imparare di più su un comando Unix, sulla sua funzionalità e/o la sua sintassi, è possibile trovare tutto questo nella corrispondente man page del programma. In Mac OS X, è possibile caricare la man page di un programma semplicemente utilizzando la sintassi:

```
man nameofcommand
```

Ad esempio, se si desidera ottenere maggiori informazioni sul comando chmod, digitare la seguente richiesta nella finestra del Terminale:

```
man chmod
```

Mac OS X visualizza le sue man page utilizzando il programma less, un semplice programma di visualizzazione del testo. Quando si preme Return dopo aver digitato una richiesta man, lo schermo del Terminale visualizza il testo corrispondente al comando in questione. Dato che il testo è in programma less, si utilizza la barra spaziatrice per far progredire il testo e si digita q per chiudere il programma di visualizzazione. Se avete seguito l'esempio e aperto la pagina man per il comando chmod, si può vedere che ci sono pagine di informazioni, molte opzioni avanzate, e anche esempi di cose che si possono fare.



Decifrare le man pages di Unix può essere un po' scoraggiante. Esse possono essere in forma molto succinta, fino al punto di essere prive di senso, e appaiono complicate al punto di poterle considerare inutili. Tuttavia non occorre davvero preoccuparsi, la cosa importante da capire è che tutte le pagine man sono basate su semplici sintassi del comando Unix che abbiamo appena discusso. Mantenere la sintassi command-name options arguments in mente consente di utilizzare esclusivamente i comandi di lettura su di loro nelle loro pagine man.

La buona notizia è che molte man pages possono essere lette e comprese, e questo è un buon punto di partenza per decifrarne altre. Con un po' di pratica si potranno leggere le informazioni delle man page senza grandi difficoltà. Si tratta, come in tutte le cose, solo di iniziare.

Se non si conosce l'esatto nome del comando, ma si sa cosa si sta cercando di fare, è possibile fare una ricerca per la man page con parole chiave. Se si desidera provare a montare un volume afp e non si è a conoscenza del programma mount_afp il, lo si può provare digitando man-k afp per avviare una ricerca con parola chiave delle pagine man per il termine "afp".

C'è da essere sicuri che, l'ultimo è mount_afp . Alcune persone *preferiscono usare il comando* apropos al posto di man-k, ma entrambi realizzano il medesimo obiettivo.

CANCELLARE UN FILE OSTINATO

A volte, il Finder non è in grado di spostare o eliminare file che si trovano nel cestino.

Il messaggio di errore "L'operazione non può essere completata perché non si dispone di privilegi sufficienti per alcuni degli elementi" appare spesso. In questo caso, ci sono due opzioni della riga di comando che è possibile utilizzare per rimuovere permanentemente i file. Il primo modo è quello di usare rm. Utilizzare la seguente procedura per provare entrambe le opzioni: Come prima cosa, provare la semplice eliminazione dei file, usando sudo per avere privilegi di root utilizzati per l'operazione.

1. Digitare sudo rm-f nome file (o sudo rm-rf nome cartella se si tratta di una cartella). sudo quindi richiede di usare la propria password.

2. Digitare la password, e al prompt si deve premere return. Se non vi è alcun errore, il file è stato rimosso.

Se la procedura fallisce, è a causa di una "flag" speciale del file, che è stata impostata sul file e i marchi per il sistema come bloccata o protetta.

In primo luogo, si rimuove la flag, e poi si rimuove il file.

1. Digitare sudo chflags-R nouchg nome del file. Dopo aver digitato la propria password, al prompt premere return.

2. Ora digitare sudo rm nome file per rimuovere il file. Se si vuole semplicemente posizionare il file nel cestino e cancellarlo in un secondo momento, è ora possibile utilizzare il Finder per mettere il file nel cestino.

Massimiliano Rinaldi
redazione@hackerjournal.it

LA POSTA IN PHP

INTERNET

VOLETE ORGANIZZARE UNA NEWSLETTER O IMPLEMENTARE INFORMAZIONI DA INVIARE VIA POSTA DAL VOSTRO SITO INTERNET? BASTA SFRUTTARE LA FUNZIONE MAIL DI PHP CON POCHE RIGHE DI PROGRAMMAZIONE.

Se abbiamo l'intenzione di creare siti web dinamici, potremmo trovarci di fronte alla necessità di inviare mail per comunicare dei dati, ad esempio confermare alcune scelte del navigatore, informare su nuovi contenuti, o mettere in collegamento fra loro due navigatori.
Prendiamo in considerazione una delle funzionalità più utilizzate in caso di segnalazioni, richieste informazioni, ordini e altro all'interno di un sito Web: la creazione di un messaggio di posta.
A questo scopo PHP mette a disposizione la funzione mail(), in grado di inviare messaggi e-mail con codifica MIME. La funzione mail() permette quindi l'invio di messaggi anche molto complessi.

MAIL, SPEDIZIONE DI UN MESSAGGIO DI POSTA ELETTRONICA

La sintassi di mail è:

```
$esito = mail($destinatario,
$oggetto, $messaggio, $altro)
```

dove:
* $destinatario è la stringa dell'indirizzo destinatario.
* $oggetto è la stringa che rappresenta l'oggetto del messaggio.
* $messaggio è il corpo del messaggio.
* $altro è una stringa (in realtà se ne possono specificare diverse) che rappresenta dei campi addizionali in un messaggio di posta elettronica compatibili con il protocollo SMTP.
* in $esito otteniamo il risultato della creazione del messaggio, che può essere vero o falso.

VEDIAMO UN SEMPLICE ESEMPIO:

```
mail.php
#!/usr/bin/php -q

$esito = mail("[nohide]
info@dominioposta.com[/
nohide]","Articolo di
PHP","Questo e' un messaggio
di prova!");
if ($esito)
echo "Ho mandato
l'email!!!\n";
else
echo "Non sono riuscito a
mandare l'email!!\n";
?>
```

DESTINATARI MULTIPLI

E' sufficiente inserire più indirizzi separati da una virgola per spedire la solita mail a più destinatari, tuttavia la procedura è sconsigliabile perché tutti potrebbero vedere gli indirizzi internet a cui spedite la mail.
Per questo motivo suggeriamo di inserire gli indirizzi in un array, oppure in un database e di inserire la funzione mail dentro un ciclo while o for, variando ogni volta la variabile del destinatario.
In pratica il funzionamento che adottano le newsletter.

di Spirit
redazione@hackerjournal.it

NAGIOS: LA RETE AZIENDALE SOTTO CONTROLLO

RETI

ALLA SCOPERTA DI UN OTTIMO STRUMENTO OPEN SOURCE DI MONITORAGGIO DEI SERVIZI DI UNA INTRANET.

Dai numerosi sondaggi e ricerche che compaiono su internet si desume che si sta andando sempre più verso l'integrazione di servizi e sistemi ogni giorno più complessi. Anche le piccole aziende si stanno dotando di server aziendali dove vengono installate applicazioni e servizi per i clienti e i propri dipendenti. Spesso però si pensa solo all'implementazione e non al controllo degli stessi server che fanno il core bussiness dell'azienda. Le capacità tecniche per fare le integrazioni ci sono ma quello che manca a mio avviso è la cultura dirigenziale per poter proporre o pensare di implementare oltre ai servizi anche un buon monitoraggio degli stessi. Un altro problema che riscontro è la paura da parte dei commerciali delle diverse aziende d'informatica, con cui sono venuto a contatto, di proporre o vendere soluzioni basate su prodotti OpenSource *perchè non c'è dietro una società o struttura tecnica di supporto* al prodotto. Le aziende si rivolgono alle società che vendono software senza pensare che non esistono solo dei software a pagamento che si occupano di fare monitoraggio dei servizi, ma ne esistono di ottimi anche Open-Source. In questa trattazione parleremo di un monitoraggio attivo/passivo e vedremo come implementarlo usando Nagios (http://www.nagios.org), un programma OpenSource per monitorare servizi e server in una realtà distribuita.

CHE COSA È NAGIOS?

Nagios® è un' applicazione per monitorare sistemi e reti, il programma controlla host e servizi che sono stati specificati nel file di configurazione e manda un alert quando questi *non sono raggiungibili oppure non* rispondono. Descritto in questo modo potrebbe sembrare un programa banale, ma non lo è, se decidete di continuare con la lettura vi accorgerete di quante cose si possono fare con Nagios e di come le fa bene, purtroppo lo spazio è tiranno e non avrò la possibilità di descrivere bene tutto il prodotto.

Nagios è stato progettato per lavorare con il sistema Operativo Linux, ma funziona bene anche con altri sistemi operativi like unix. Tra i numerosi servizi che possono essere controllati da Nagios® ci sono:
Monitoring di servizi di network (SMTP, POP3, HTTP, NNTP, etc.)
Monitoring di risorse dei server (carico della CPU, uso dei dischi, esistenza di un processo, etc.)
Monitoring di raggiungibilità(PING)
La semplicità dei plugin, inoltre, permette di sviluppare facilmente dei nuovi ceck per i propri servizi. Tutti i controlli, anche quelli implementati *ex novo come per quelli di default*, possono essere effettuati in parallelo. Una delle caratteristiche peculiari di Nagios® è la possibilità di definire la "network host hierarchy" usando una parentela tra gli host, "parent". In questo modo si disegna la rete e si può fare una diagnosi veloce in caso di problemi distinguendo tra hosts che sono down e quelli che sono







irraggiungibili. Le notifiche, quando un host ha un problema oppure è stato risolto, possono avvenire in diversi modi: via email, via pager, o qualsiasi altro metodo definito dall'utente. E' prevista inoltre la possibilità di far eseguire degli script di risposta all'evento "down" come all'evento "up". La possibilità di far generare delle risposte automatiche al programma al succedersi di certi eventi rende il sistema oltre che di monitoraggio un sistema di risposta proattiva limitando il disservizio verso l'utente finale.

REQUIREMENTS

L'unica cosa che serve per fa girare Nagios è una macchina che abbia come sistema operativo Linux (o una variante UNIX) e un compilatore C. La configurazione del protocollo TCP/IP è necessaria per poter controllare i servizi di rete e i server remoti. Non è necessario usare le CGI che fanno parte del pacchetto Nagios, ma se si vogliono implementare bisogna configurare il web server per l'esecuzione delle CGI. Noi in questa trattazione prenderemo in considerazione il web server Apache. Un altro pacchetto non necessario ma utile per la visualizzazione grafica è la "Thomas Boutell's" libreria, la gd version 1.6.3 o superiore. Questa libreria, utilizzata soprattutto insieme ad Apache, serve per la creazione dinamica di immagini in formato PNG e JPEG, Nagios la usa per creare le mappe ed i grafici di raggiungibilità dei server.

INSTALLAZIONE

A differenza dei programmi a cui siamo abituati normalmente nel mondo OpenSource compilare e installare Nagios non basta per poi vederlo al lavoro eseguendolo. Esistono una serie di configurazioni che devono essere effettuate prima di avere una console di monitoraggio funzionante e funzionale. Partiremo da un server Linux con Sistema operativo RedHat e assumeremo che Nagios verrà installato nella directory /usr/local/nagios e che sia configurato Apache per usare le CGI, l'installazione che faremo si aspetterà che le CGI di nagios siano accessibili all'url htt://localhost/nagios/cgi-bin/. Se così non fosse si può usare l'opzione --with-cgiurl con lo script configure per modificare il path delle CGI.
La prima cosa da fare è scaricare il programma dal sito ufficiale insieme ai plugin, poi seguendo la documentazione si può passare all'installazione ed alla configurazione dei servizi da monitorare.
Vediamolo passo passo:
Una volta scaricato il pacchetto va scompattato in una directory temporanea con il consueto comando

```
# tar cvfz nagios.1.x.tgz
```

entrare nella directory con il comando cd nagios.1.x/ e leggere il README e INSTALL. Prima di proseguire con l'installazione creiamo l'utente con cui faremo girare il programma con i comandi che seguono:

```
# adduser nagios
```

poi eseguiamo lo script di configurazione con i parametri necessari al nostro ambiente di lavoro:

```
# ../configure --prefix=PREFIX
--with-cgiurl=CGIURL --with-
htmurl=HTMURL  \
--with-nagios-user=SOMEUSER
--with-nagios-grp=SOMEGROUP
```

a) Cambiare PREFIX con la directory dove dovrà essere installato Nagios, di Default viene usata la directory '/usr/local/nagios'

b) Cambiare CGIURL con l'URL che deve essere usata per raggiungere le CGI. Non mettere lo slash finale. Il default è '/nagios/cgi-bin'

c) Cambiare HTMURL con l'URL che deve essere usata per accedere alle pagine di documentazione html ed alla pagina principale di Nagios. Il default è '/nagios'

d) Cambiare SOMEUSER con il nome dell'utente, esistente sul proprio sistema, da essegnare come proprietario dei file e delle directory di Nagios. Il default è 'nagios'

e) Cambiare SOMEGROUP con il nome del gruppo, esistente sul proprio sistema, da associare a tutti i file come proprietario di essi. Il default è 'nagios'
ora compiliamo e installiamo il programma:

```
# make all
# make install
# make install-config
```

per ultimo, se la compilazione è andata a buon fine, installiamo lo script di inizializzazione che va a finire nella directory /etc/init.d:
make install-init
lo script va poi editato per effettuare le modifiche relative al nostro ambiente di lavoro, se abbiamo lasciato tutte le configurazioni standard queste ultime non servono, va solo personalizzata la parte relativa la nostro Sistema Operativo come la variabile PATH ecc.
Finita l'installazione vediamo che cosa abbiamo nelle sotto directory del programma che si trova nella directory /usr/local/nagios:

bin/ Nagios programma principale
etc/ Directory dove troviamo i file di configurazione installati con il comando make install-config

sbin/ CGI usate da Nagios
share/ file HTML (per l'interfaccia web e la documentazione ufficiale)
var/ directory vuota per i log file

INSTALLAZIONE DEI PLUGINS

I plugins che si possono usare con Nagios sono tanti, questi possono essere scaricati dal sito ufficiale che è http://nagiosplug.sourceforge.net Dopo aver fatto il download e aver scompattato il file bisogna entrare nella directory e lanciare il comando configure, seguito dal comando di compilazione Make.

```
# ./configure
# make
# make install
```

SETTAGGIO DI APACHE

Dopo aver installato il programma anche prima di aver configurato i server da monitorare, provvederemo alla configurazione di Apache per poter accedere via browser alla console di Nagios ed a tutta la documentazione. Bisogna aggiungere un alias e aggiungere la directory degli script CGI. La configurazione per Nagios si può includere in un file che verrà caricato dal file principale di Apache con la direttiva Include.
La modifica da apportare al file di configurazione di Apache dovrebbe assomigliare a quella riportata sotto:

```
ScriptAlias /nagios/cgi-bin/
/usr/local/nagios/sbin/
<Directory "/usr/local/
nagios/sbin/">
    AllowOverride AuthConfig
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>
Alias /nagios/ /usr/local/
nagios/share/
<Directory "/usr/local/
nagios/share">
    Options None
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

La parte di ScriptAlias deve precedere la parte Alias altrimenti Apache fa il parsing in maniera diversa e non trova le CGI.
Dopo aver modificato il file di configurazione di Apache per vedere gli effetti della modifca bisogna riavviare il servizio web con il consueto comando:

```
# /etc/init.d/httpd restart
```

che è uguale al comando :

```
# service httpd restart
```

METODI PER LANCIARE NAGIOS

Nagios può essere lanciato in diversi modi. I metodi classici sono quattro:

Manualmente, come processo in foreground (di solito per i test iniziali)
`/usr/local/nagios/bin/nagios <main_config_file>`

Manualmente, come processo in background.
`/usr/local/nagios/bin/nagios <main_config_file> &`

Manualmente, come processo demone
`/usr/local/nagios/bin/nagios -d <main_config_file`

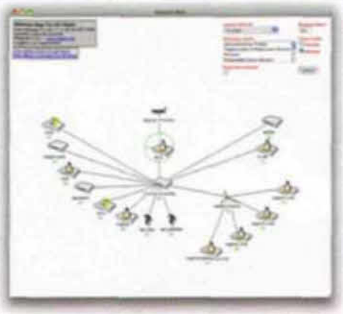
Automaticamente al boot.
Se abbiamo lanciato dopo l'installazione del programma il comando
'make install-init
allora abbiamo installato anche lo script per l'avvio automatico al boot.

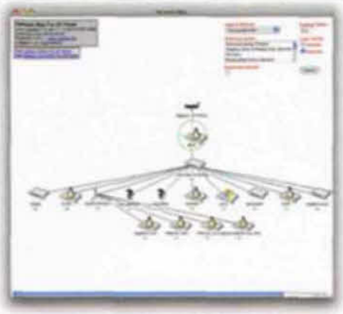
A questo punto se il nostro processo è in esecuzione puntando il browser all'indirizzo http://localhost/nagios si può accedere all'interfaccia web principale di Nagios che oltre alla documentazione presente nella directory /usr/local/nagios/share, che è anch'essa consultabile via web, permette di avere un quadro completo della rete monitorata.
Una precauzione da prendere se si usa Nagios per monitorare servizi direttamente su Internet è l'accesso alle pagine di visualizzazione di Nagios tramite password, questo prevede di configurare Apache per far accedere gli utenti tramite login e password. Come abbiamo accennato sopra bisogna ora pensare alle altre configurazioni e definire i server ed i servizi da tenere sotto controllo.

CONFIGURAZIONE E DISEGNO DELLA MAPPA DI RETE

La prima cosa da fare è avere un elenco aggiornato dei server e dei servizi su ogni singolo server. Questo elenco ci servirà per costruire il nostro file di configurazione da dare in pasto al programma che farà i controlli.
Il file principale per configurare Nagios è:

```
/usr/local/nagios/etc/nagios.
cfg
il file è commentato ed
autoesplicativo, inoltre
all'interno si trova
l'elenco degli altri file di
configurazione che sono:
/usr/local/nagios/etc/hosts.
cfg
/usr/local/nagios/etc/
checkcommands.cfg
/usr/local/nagios/etc/
contacts.cfg
/usr/local/nagios/etc/
contactgroups.cfg
/usr/local/nagios/etc/
hostgroups.cfg
/usr/local/nagios/etc/
services.cfg
/usr/local/nagios/etc/
timeperiods.cfg
/usr/local/nagios/etc/
escalations.cfg
/usr/local/nagios/etc/
misccommands.cfg
```







ogni file è commentato e seguendo gli esempi si possono modificare per raggiungere il nostro scopo. Questo ci permette di rendere operativo il programma velocemente.

VERIFICA DEL FILE DI CONFIGURAZIONE

Dopo aver finito la parte di configurazione bisogna provare e testare se tutto funziona, si può lanciare Nagios con il flag -v per vedere se i file di configurazione stanno a posto:

```
/usr/local/nagios/bin/nagios
-v <config_file>
```

config_file è il file dove abbiamo fatto le configurazioni, Nagios verifica se è tutto ok senza lanciare il monitoraggio.
Verifica che tutti i contatti siano membri di almeno un contact group.
Verifica che tutti i contatti specificati in ogni contact group siano validi.
Verifica che tutti gli hosts siano membri di almeno un host group.
Verifica che tutti gli hosts specificati in ogni host group siano validi.
Verifica che tutti gli hosts abbiano almeno un servizio associato da monitorare.
Verifica che tutti i comandi usati per controllare gli host ed i servizi siano validi.
Verifica che tutti i comandi usati in service and host event handlers siano validi.
Verifica che tutti i comandi usati in contact service and host notifications siano validi.
Verifica che tutti i periodi temporali specificati per services, hosts, e contact siano validi.
Verifica che tutti i periodi temporali specificati per services siano validi.
Se i file di configurazione sono giusti allora si può proseguire con il nostro monitoraggio e vedere come si comporta Nagios, se invece ci viene segnalata un'errata configurazione si può modificare il file e riprovare.

USO DI NAGIOS E REPORT

Dopo aver completato la nostra configurazione e settaggio della console degli eventi, si ha a disposizione uno strumento di prevenzione e di monitoraggio che aiuta il normale lavoro del sistemista. Inoltre se diamo un'occhiata nella parte sinistra del browser troviamo oltre al link alle diverse pagine di monitoraggio attivo i link ai report. Poichè Nagios colleziona gli eventi e li registra in un file questi si possono aggregare per fornire statistiche e grafici in tempo reale di quello che è successo nella nostra rete al cliente o al responsabile del servizio. Se questo non serve per avere sotto controllo il lavoro da fare può servire per cercare di capire se si può migliorare il tempo di risposta ai problemi oppure se si può intervenire in altri modi e far sì che il disservizio sia minimo nei confronti degli utilizzatori finali.
Nonostante io usi Nagios da diversi anni, ho iniziato ad installarlo quando si chiamava "Netsaint", e ritenendolo un ottimo prodotto, riporto sotto un elenco di software che fanno monitoring o si occupano di fornire un ottimo aiuto in un ambiente distribuito, a qualcuno può far comodo avere un elenco a portata di mano. Queste utility si possono trovare facilmente su Internet, per alcuni riporto direttamente il link, gli altri si possono reperire utilizzando i motori di ricerca specializzati in software.

Utility di Monitoring tratte direttamente dalla documentazione di Nagios

Angel Network Monitor http://www.paganini.net/angel/
Autostatus
http://www.angio.net/consult/autostatus/
HiWAyS
http://www.hiways.org/
MARS
http://www.altara.org/mars.html
Mon
http://www.kernel.org/software/mon/
Netup (French)
NocMonitor
NodeWatch
Penemo
http://www.penemo.org/
PIKT
http://pikt.org/
RITW
Scotty
Spong
Sysmon

Bibliografia e link
Sito principale di Nagios http://www.nagios.org
Download dei plugins http://nagiosplug.sourceforge.net



di Spirit
redazione@hackerjournal.it

EXPLOIT E DINTORNI

Questa nuova sezione di Security Lab (il nostro inserto dedicato in modo mirato ai temi della sicurezza, lanciato a partire da questo numero) è dedicata ai malware, exploit e attacchi che si sono guadagnati l'onore delle cronache nell'ultimo mese.

Downloader.JS.Pegel.b

Una menzione di merito spetta al Trojan Downloader.JS.Pegel.b. Questo script downloader, progettato per infettare i siti web, si è rivelato tra i più diffusi dopo un periodo di relativa inattività. Quando un utente visita una pagina infetta, Pegel li reindirizza a un sito controllato da un criminale informatico, che a sua volta scarica programmi maligni nel computer della vittima. Pegel.b fa uso di exploit PDF e Java CVE-2010-0886.

Exploit.JS.Pdfka

Il rilascio di ogni nuovo aggiornamento di Adobe è sempre accompagnato da diverse varianti di questo exploit. Nel solo mese di giugno, tre varianti di Exploit.JS.Pdfka sono entrate nella classifica dei malware Internet rispettivamente al sesto, ottavo e quattordicesimo posto.

Agent.bab

E' stato uno dei malware più diffusi dell'ultimo periodo. Sfrutta la vulnerabilità di Windows CVE-2010-0806, rilevata a marzo di quest'anno, per scaricare diversi programmi dannosi nei computer degli utenti. A giugno il numero di singoli tentativi di scaricare questo malware da siti internet ha superato le 340.000 unità.

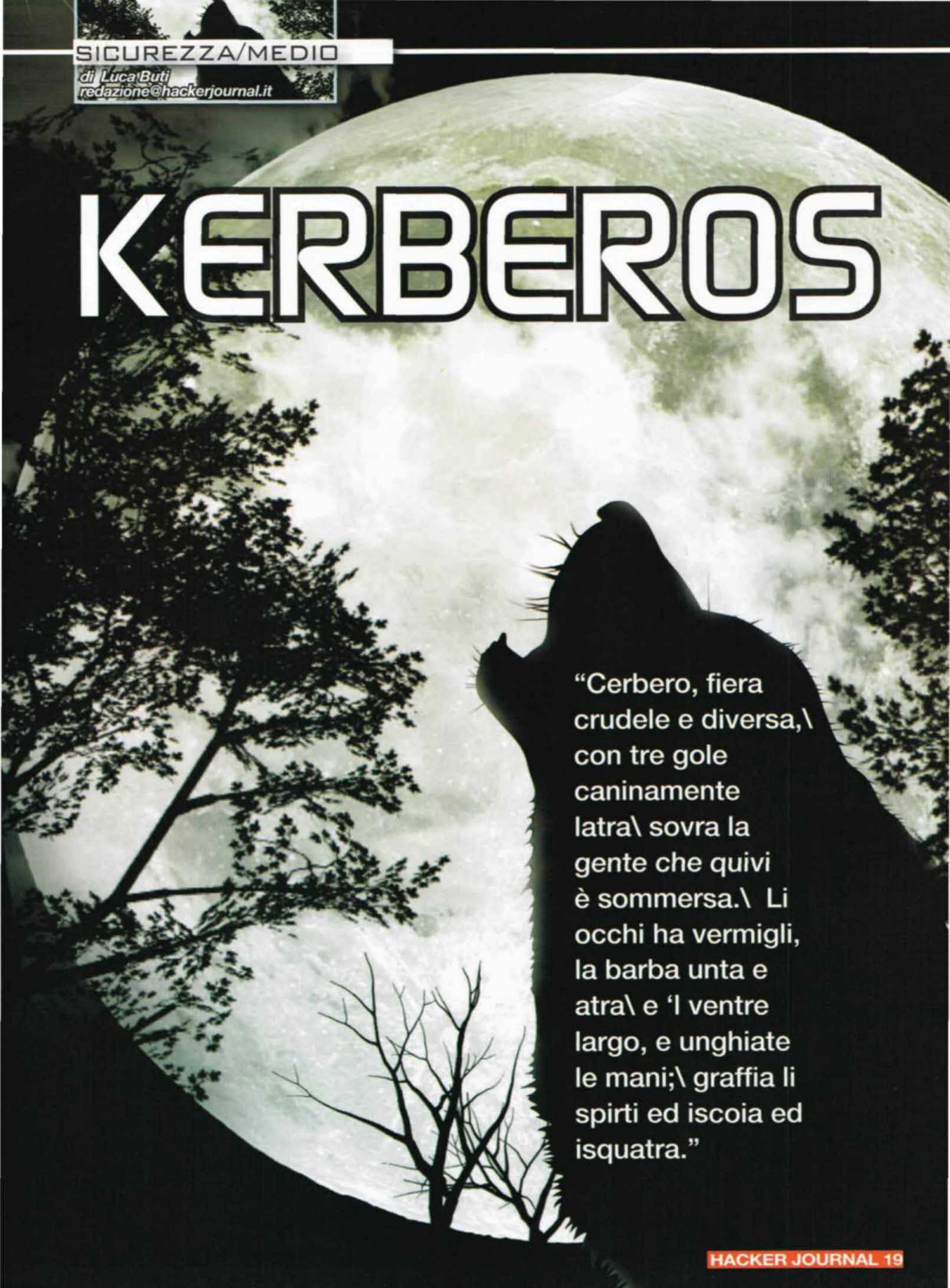
P2P-Worm.Palevo

Per la maggior parte dei criminali informatici, i dati riservati sono fonte di grandi guadagni: una nuova variante del popolare P2P-Worm.Palevo cerca appunto di rubare dati sensibili penetrando attraverso una finestra del browser degli utenti. Questo worm si propaga utilizzando programmi Peer-to-peer di file sharing come BearShare, iMesh, Shareaza e eMule. Esegue più copie di se stesso nelle cartelle utilizzate per memorizzare i file che sono comunemente scaricati e caricati, dando nomi accattivanti ai file infetti nella speranza che possano attirare l'attenzione di potenziali vittime. Altri mezzi con cui si propaga P2P-Worm.Win32.Palevo.fuc comprendono la riproduzione di più copie di cartelle e risorse di rete, l'invio di link via instant messenger e il Trojan.Win32.Autorun che può infettare qualsiasi tipo di dispositivo rimovibile con cui entra in contatto.

AdWare.Win32.FunWeb.ds

Raccoglie dati sulle richieste di ricerca degli utenti e, spesso, questi dati vengono poi utilizzati da un sistema per visualizzare dei banner che frequentemente compaiono durante la navigazione on-line.

di Luca Buti
redazione@hackerjournal.it



KERBEROS

"Cerbero, fiera crudele e diversa,\ con tre gole caninamente latra\ sovra la gente che quivi è sommersa.\ Li occhi ha vermigli, la barba unta e atra\ e 'l ventre largo, e unghiate le mani;\ graffia li spirti ed iscoia ed isquatra."



Questo passo, tratto dal quarto canto della Divina Commedia di Dante, descrive Cerbero, in inglese Kerberos, il mitico cane a tre teste pena dei golosi.
Nel campo dell'informatica, questa bestia mitologica è stata utilizzata come nome e simbolo di un noto protocollo per l'autenticazione dei servizi di rete, il Kerberos, contraddistinto da un'architettura definita three-sided. Questo termine significa che il protocollo utilizza tre componenti per raggiungere il suo obiettivo di spedizione affidabile dei dati attraverso una rete: uno di essi è il client, che rappresenta l'utente, il secondo è il server, al quale si richiede l'accesso ed il terzo è un contenitore delle informazioni riguardanti le chiavi d'accesso.
Per comprendere meglio come funziona il sistema, dobbiamo tornare indietro negli anni '80, quando Kerberos venne creato nei laboratori del Massachusetts Institute of Technology, probabilmente il più famoso centro di ricerca tecnologica del mondo. A quei tempi l'autenticazione degli utenti, necessaria per fornire servizi di rete, avveniva attraverso la richiesta e l'invio di username e password, ed il suo trasporto era "in chiaro". Questo significa che era possibile, e per alcuni servizi lo è ancora, carpire le password spedite semplicemente "ascoltando" lo scambio di dati tra server ed utente.
Per alcuni servizi, come il classico telnet, le password sono spedite ancora senza nessun algoritmo di crittografia, rendendo il loro uso altamente sconsigliato in ambiti nei quali la sicurezza è necessaria. L'operazione di ascolto di un traffico di rete si chiama packet sniffing, ed è talmente facile da sfruttare che anche una persona poco esperta e male intenzionata potrebbe farne uso.

CHIAVI DI CRITTOGRAFIA

Una soluzione molto utilizzata per risolvere il problema è l'uso di protocolli sicuri che sfruttino lo scambio di chiavi di crittografia e spediscano i dati in maniera cifrata, come per esempio fa ssh.
Nei laboratori del MIT si studiò un sistema in grado di permettere lo scambio sicuro delle informazioni di autenticazione per vanificare eventuali tentativi di ascolto del traffico, allo scopo di ottenere dati di accesso validi. Per funzionare, come abbiamo già accennato, Kerberos utilizza tre componenti, client, server e KDC (Key Distribution Center).
All'atto dell'autenticazione è richiesto un Ticket, una sorta di biglietto d'entrata che permette l'accesso al servizio per una sessione ad un determinato utente. Quando un utente cerca di connettersi ad una workstation che sfrutta una rete autenticata con Kerberos, viene inviato un messaggio al KDC che richiede un TGT (Ticket Granting Ticket), un biglietto che permette di ottenere altri ticket senza doverli richiedere nuovamente al KDC.
Il messaggio inviato contiene il Principal, che è un utente o un servizio che può essere autenticato tramite Kerberos ed ha l'identificativo in questa forma:

```
root[/instance]@REALM
```

Il Realm è la definizione nella terminologia di Kerberos di una rete basata su questo sistema. Esso può essere costituito da più KDC e da un insieme arbitrario di client e server.

Il Kdc controlla l'esistenza del principal nel suo database, e, nel caso riesca a trovarlo, prepara un Tgt cifrandolo con la chiave dell'utente ed inviandolo a chi ne ha fatto richiesta. A questo punto il client decifra il Tgt utilizzando la chiave dell'utente, ricavata dalla password inserita, e la memorizza per un tempo variabile e limitato, durante il quale l'utente non ha solitamente bisogno di reinserire la sua password.
Quando l'utente ha bisogno di autenticarsi per un servizio, il client richiede al Ticket Granting Service il ticket utilizzando il biglietto Tgt. Spesso il Kdc ed il Tgs coincidono e si trovano sulla stessa macchina fisica, per risparmiare sui costi di gestione. Abbiamo accennato al fatto che i Ticket Granting Ticket hanno una durata, entro la quale l'utente non deve reinserire nuovamente la password.

Questa caratteristica introduce un problema di sicurezza non banale: se il computer client ed il server Kdc non sono sincronizzati, un utente malizioso potrebbe usare ticket scaduti per accedere a servizi a lui negati. Per questo motivo, quando si configura una rete basata su Kerberos, dobbiamo preoccuparci di avere tutte le macchine sincronizzate, con uno scarto massimo standard di cinque minuti, che eventualmente si può rimodellare secondo le nostre esigenze. Per farlo, possiamo utilizzare il Network Time Protocol, che fornisce una sincronizzazione automatica grazie ad un demone chiamato ntpd.

Esso è contenuto nel pacchetto ntp, ed è disponibile sia sui cd delle maggiori distribuzioni che su internet in vari indirizzi, tra i quali rpmfind.net. Per installarlo su una Debian si usa il comando:

```
# apt-get install ntp
```

Mentre per le distribuzioni basate su rpm bisogna prima scaricare il pacchetto e poi installarlo con il solito:

```
# rpm -ivh ntp-versione.rpm
```

Possiamo configurarlo sia agendo sul file /etc/ntp.conf che con il programma disponibile in Red Hat chiamato

```
# redhat-config-date
```

7In entrambi i casi dovremo specificare un server di riferimento con il quale sincronizzare il nostro pc, ed una lista di quelli pubblici può essere trovata all'indirizzo: www.eecis.udel.edu/~mills/ntp/servers.html.
Il file di configurazione /etc/ntp.conf è mostrato nella Tabella 1, e l'unica cosa che dovremo fare è accertarci che tutti i file di configurazione dei pc, che costituiscono la nostra rete Kerberos, utilizzino gli stessi campi nella voce server, per averli tutti sincronizzati sulla stessa ora.

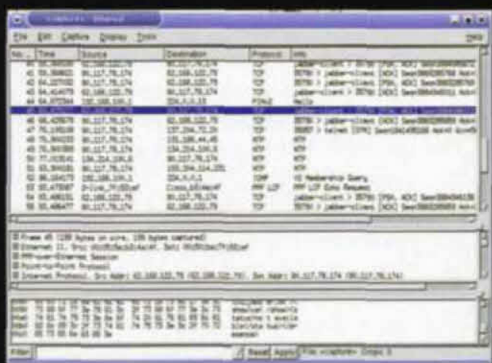


TABELLA 1:
Il file /etc/ntp.conf

```
# /etc/ntp.conf, configuration for ntpd
# ntpd will use syslog() if logfile is not defined
# logfile /var/log/ntpd
driftfile /var/lib/ntp/ntp.drift
statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
# sezione dedicata ai server per la sincronizzazione, è importante che
# tutti i pc delle stessa LAN usino gli stessi indirizzi ip.
server 193.204.114.231

server 131.188.44.45

server 134.214.100.6
```

Ora che siamo sicuri che tutti i pc della rete Kerberos sono stati sincronizzati, dobbiamo accertarci che sia ben configurato il Dns nella macchina che farà da server Kdc. Procediamo quindi con l'installazione dei pacchetti necessari nel server, utilizzando la distribuzione Red Hat come piattaforma di base. Sarà facile trasportare le stesse nozioni anche su macchine con installate altre distribuzioni, perciò lasciamo al lettore il compito di adattare le soluzioni di questo articolo alle esigenze personali.

Per prima cosa installiamo i pacchetti krb5-libs, krb5-server, krb5-workstation. Dopo aver installato il software necessario dobbiamo decidere come chiamare il nostro Realm. Una convenzione molto usata è quella di utilizzare lo stesso nome del dominio, utilizzando però solo lettere maiuscole, come ad esempio HACKERJOURNAL.IT per il dominio hackerjournal.it.
I due file di configurazione da modificare sono /etc/krb5.conf e /var/kerberos/krb5kdc/kdc.conf
Potete vedere un esempio di come vanno configurati questi due file nelle Tabelle 2 e 3. Ovviamente dovete sostituire ad "esempio.com" il vostro dominio, e ad "ESEMPIO.COM" il vostro Realm. Dovete fare attenzione a non scambiare per errore maiuscole e minuscole, perché in questa situazione hanno diversi significati.

TABELLA 2:
Esempio di file /etc/krb5.conf

```
[logging]
```

```
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 ticket_lifetime = 24000
 default_realm = ESEMPIO.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false

[realms]
 ESEMPIO.COM = {
 kdc = kerberos.esempio.com:88
 admin_server = kerberos.esempio.com:749
 default_domain = esempio.com
 }

[domain_realm]
 .esempio.com = ESEMPIO.COM
 esempio.com = ESEMPIO.COM

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
}
```

TABELLA 3: Esempio del file di configurazione /var/kerberos/krb5kdc/kdc.conf

```
kdcdefaults]
 acl_file = /var/kerberos/krb5kdc/kadm5.acl
 dict_file = /usr/share/dict/words
 admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
 v4_mode = nopreauth

[realms]
 ESEMPIO.COM = {
 master_key_type = des-cbc-crc
 supported_enctypes = des3-cbc-sha1:normal des3-cbc-sha1:norealm des3-cbc-sha1:onlyrealm des-cbc-crc:v4 des-cbc-crc:afs3 des-cbc-crc:normal des-cbc-crc:norealm des-cbc-crc:onlyrealm des-cbc-md4:v4 des-cbc-md4:afs3 des-cbc-md4:normal des-cbc-md4:norealm des-cbc-md4:onlyrealm des-cbc-md5:v4 des-cbc-md5:afs3 des-cbc-md5:normal des-cbc-md5:norealm des-cbc-md5:onlyrealm des-cbc-sha1:v4 des-cbc-sha1:afs3 des-cbc-sha1:normal des-cbc-sha1:norealm des-cbc-sha1:onlyrealm
}
```

Dopo aver inserito i nostri dati nei due file di configurazione principali del server KDC, dobbiamo creare il database che conterrà le chiavi, tramite il comando:

```
# /usr/kerberos/sbin/kdb5_util create -s
```

L'opzione -s serve per immagazzinare la chiave del server in un file e se non specificata occorrerà reinserirla ad ogni reboot del server. Una volta creato il database delle chiavi, dobbiamo stabilire quali principal avranno permesso di modificare il database delle chiavi di kerberos, agendo sul file di configurazione /var/kerberos/krb5kdc/kadm5.acl. Solitamente in questo file basterà inserire questa unica linea:

```
*/admin@ESEMPIO.COM *
```

la quale indica al server Kerberos che qualsiasi utente che abbia un'istanza di admin nel realm ESEMPIO.COM, possiede anche pieni poteri sul database. Le istanze, come al solito, vengono indicate nel principal in un modo simile a questo:

max/admin@ESEMPIO.COM

dove la voce prima dello "/" indica l'utente, la stringa compresa tra lo slash e la chiocciola indica l'istanza, e la parte finale indica il Realm.

KADMIN

Per amministrare i principal si utilizzerà il programma kadmin, che si connette al demone kadmind utilizzando un'autenticazione Kerberos. Ovviamente per poterlo utilizzare l'amministratore dovrà creare almeno un Principal di partenza, con il quale potrà successivamente eseguire kadmin. Per creare il primo principal, basterà eseguire il comando:

```
# /usr/kerberos/sbin/kadmin.local -q "addprinc max/admin"
```

Il comando kadmin.local si usa solamente nello stesso host del Kdc e non utilizza l'autenticazione su Kerberos, che, d'altra parte, non sarebbe ancora disponibile a causa dell'assenza di principal nel database. Lo stesso comando si può utilizzare per aggiungere altri utenti, come ad esempio:

```
# /usr/kerberos/sbin/kadmin.local -q "addprinc max"
```

L'utente appena creato non possiede un'istanza di admin ed è considerato quindi un utente standard. Dopo aver aggiunto gli utenti, dovremo far partire i demoni per Kerberos:

```
# /etc/init.d/krb5kdc start
# /etc/init.d/kadmin start
# /etc/init.d/krb524 start
```

Per farli partire automaticamente ad ogni avvio possiamo utilizzare il programma chkconfig:

```
# chkconfig --level 345 krb5kdc on
# chkconfig --level 345 kadmin on
# chkconfig --level 345 krb524 on
```

Abbiamo quindi terminato la configurazione del server. Prima di passare ai client è necessario porre attenzione ancora su qualche aspetto di sicurezza. Data la centralità del sistema di autenticazione Kerberos, è *indispensabile per un amministratore* avere la certezza che la macchina che funge da Kdc sia protetta contro accessi non autorizzati.

I comandi che abbiamo appena visto possono permettere ad un intruso di creare un personal e conseguentemente di avere accesso a tutti i computer che fanno uso dell'autenticazione Kerberos. *Inoltre, la sicurezza di questo* sistema si estende solo ai programmi che fanno uso dell'autenticazione Kerberos, quindi dovremo sostituire i programmi insicuri con applicativi che offrono già il supporto a questo sistema. Inutile dire che se un utente utilizza il classico telnet, lascia che la sua password venga trasmessa in chiaro. Se questa disgraziatamente è la stessa utilizzata per Kerberos, *allora il suo account è compromesso* indipendentemente dalla sicurezza del sistema del MIT.

IL CLIENT

Per proseguire con il nostro esempio di campo applicativo di Kerberos, configureremo una macchina client per supportarne l'autenticazione. Se stiamo installando da zero il client, possiamo utilizzare l'apposito pannello di configurazione che viene fornito con il setup della Red Hat : alla voce configurazione dell'autenticazione ci viene permesso di utilizzare Kerberos, scegliendo tra le tre opzioni disponibili (Accesso ad una rete che usa Kerberos, accesso ad un Kdc o accesso ad una macchina che utilizza kdamind).

Se invece dovete effettuare questo procedimento dopo la prima installazione, allora dovete assicurarvi di aggiungere i pacchetti krb5-libs e krb5-workstation, ed eseguire il programma authconfig.

In generale le operazioni da fare sono copiare il file /etc/krb5.conf in tutti i client e cambiare il file /var/kerberos/krb5kdc/kdc.conf in modo coerente. *Dopo aver creato correttamente questi* due file, dobbiamo creare un principal corrispondente all'host da aggiungere alla rete. Per fare quest'ultimo passaggio dovremo eseguire nel Kdc:

```
# kadmin
```

Che ci fornirà una console con la quale andiamo ad aggiungere l'host:

```
# addprinc -randkey host/
client1.esempio.com
```

Dove la parte successiva al "/" corrisponde al nome dell'host da aggiungere. L'opzione randkey serve a creare una chiave casuale. Dopo aver creato il principal per il client, ne estrapoliamo le chiavi:

```
# ktadd -k /etc/krb5.keytab
host/client1.esempio.com
```

Ora abbiamo a disposizione un sistema Kerberos 5 funzionante, ma dobbiamo assicurarci che i programmi utilizzino questo sistema per autenticare i loro utenti.

In generale, un'applicazione deve già essere stata pensata per un determinato sistema di autenticazione, *quindi è necessario cercare la versione* che utilizza kerberos o ricompilare i sorgenti dopo averli modificati allo scopo.

MODULI DI AUTENTICAZIONE

I moduli di autenticazione Pam *ci vengono in aiuto, fornendo un* livello di astrazione sufficiente ad evitare la ricompilazione e l'adattamento di tutte le applicazioni che li utilizzano. Per esempio, per l'accesso al sistema il file di configurazione per l'autenticazione è /etc/pam.d/login, e modificando questo file in tutti i client potremo utilizzare Kerberos per il login di sistema. Un esempio della configurazione per il login e per il servizio Ftp è mostrato nella Tabella 4.

Ovviamente dovremo configurare ogni file di configurazione della directory /etc/pam.d relativo ai servizi che vorremo autenticare attraverso Kerberos.

TABELLA 4:
Utilizzo di kerberos in /etc/pam.d/login

```
#/etc/pam.d/login

auth required /lib/security/
pam_securetty.so
auth required /lib/security/
pam_nologin.so
auth sufficient /lib/security/
pam_krb5.so
auth required /lib/security/
pam_pwdb.so shadow nullok
use_first_pass

#/etc/pam.d/ftp
auth required /lib/security/
pam_listfile.so item=user
sense=deny file=/etc/ftpusers
onerr=succeed
auth sufficient /lib/security/
pam_krb5.so
auth required /lib/security/
pam_pwdb.so shadow nullok
use_first_pass
auth required /lib/security/
pam_shells.so
```

CONCLUSIONI

Ora che abbiamo imparato come utilizzare un sistema di difesa abbastanza potente, dobbiamo *essere sicuri che ogni componente* utilizzato lo sfrutti, eventualmente eliminando gli altri sistemi di autenticazione, togliendo gli utenti dai sistemi non Kerberos ed obbligandoli quindi al suo utilizzo, magari dopo un periodo di test.

LA POSTA DI HJ

IDEE PER IL CORSO IN C

Ciao a tutti!
Sono un vostro lettore da molti anni.
Ho molto apprezzato la vostra idea di pubblicare i vecchi numeri in pdf e la proposta di un abbonamento on-line.
Volevo tuttavia consigliarvi due cose sul corso C:
- quando il corso sarà concluso perché non uscite con un volume speciale che raccoglie tutte le puntate?
- trattate anche qualche puntata sulla programmazione delle interfacce
perché penso possa essere utile, interessante e dia un tocco di qualità tipico di HJ.

Giorgio Boiero

Caro Giorgio, l'idea della raccolta ci era già venuta e la tua mail rafforza l'idea che, in effetti, non sia male. La proporremo all'editore, vediamo cosa si riesce a fare. Per quanto riguarda invece il corso in C ci sono due cose da segnalare: la prima è un gradimento (e un successo) che è andato oltre le nostre aspettative, la seconda, proprio sulla scorta del successo riportato, è quella di allungare leggermente il corso, aggiungendo una "coda" per trattare alcuni argomenti fin qui esclusi.
Riguardo gli spazi e la quantità di pagine aggiunte ci stiamo ragionando. Non saranno tantissime perché lo spazio sul giornale è ristretto ed è stato già abbondantemente "sacrificato" al corso in C nell'arco di questi mesi (ci mettiamo nei panni anche di coloro che non sono interessati al corso e saltano a piè pari le 6 pagine di ogni numero), ma un allungo quasi sicuramente ci sarà.

UNA RAFFICA DI PROPOSTE

Salve,
da qualche tempo leggo con interesse e passione la vostra rivista; secondo me è tra le poche riviste, forse l'unica che scriva cose veramente uniche, utili, e particolari riguardo al mondo informatico.
Negli ultimi due numeri ho letto riguardo al cambiamento della veste grafica e delle scelte editoriali.
Devo dirvi che le condivido in parte.
Personalmente io valuterei se intraprendere una strada completamente opposta.
Cerco di illustrarvela in breve:
1) sdoppiamento di target.
La rivista si sdoppierebbe nel senso che farei uscire due numeri di rivista per due differenti target: un numero per il "pubblico o neofiti", un altro per i più appassionati e ferrati in informatica, programmazione etc.
Nella rivista per il pubblico argomenterei ad esempio, su sistemi operativi -tutti anche per mobile e phone- pregi, difetti, come migliorare la sicurezza di una rete domestica etc., piccolo codice (in vari linguaggi) da usare per applicazioni pratiche, per crearsi piccoli giochi, etc.
Notizie dal mondo dell'informatica, software, hardware recensioni. Bello sarebbe inserire un po' di storia dell'informatica della matematica e loro risvolti sull'unanità.
Pubblicherei delle rubriche pratiche periodiche: ad esempio una rubrica A ogni mese; un'altra B ogni 3 mesi; oppure un altra C ogni Ogni 6. etc
Inserirei anche un po' di -ahi noi- pubblicità; molto scelta e mirata e poco consumistica.
Stampata in carattere gradevole, non grande o troppo piccolo, secondo il format di un rotocalco senza perdere lo stile Hackerjournal.
Un formato pratico quasi da "esibire" sempre da 32 pagine. Molto spazio a posta e problemi.
Una rivista che, tratterebbe in modo facile argomenti difficili, da leggere tutta d'un fiato ovunque (anche sotto l'ombrellone), da finire subito, e rendere quindi interminabile l'attesa per il numero del mese prossimo.
In realtà un viatico per la lettura dell'altra rivista quella per appassionati.
Per la rivista dedicata agli appassionati vanno bene le impostazioni dei numeri dal 200 in poi. Nessun compromesso codici, linguaggi di programmazione, SQL etc. Nessuna pubblicità.
2) abbonamenti
Per entrambe la rivista disponibile abbonamento tramite posta e pdf da scaricare dal sito e "pagare tramite i soliti metodi di e-commerce". Per la rivista per appassionati magari per contenere i costi delle spedizioni postali (non c'è pubblicità ricordo) si potrebbe optare per una spedizione che contenga due numeri invece che uno.
3) Diversi tempi di uscita.
La data del 23 di ogni mese è molto buona perchè non mi pare escano molte altre riviste in questa data; si potrebbe far uscire l'edizione per il pubblico.
Mentre l'edizione per appassionati potrebbe uscire verso il 7-15 di ogni mese, "quando l'attesa per l'altra edizione diventa insopportabile."
4) Grafica
Marchio più piccolo, stilizzato e 3d; qualche teschio qua e là (volendo). Va bene la struttura e lo sfondo delle pagine.

Disseminare le due edizioni di giochini in tema più o meno difficili, alcuni a pronta soluzione altri a soluzione a prossimo numero, altri senza soluzione nel senso che il gioco resta solo fino a quando

LA POSTA DI HJ

viene data la soluzione.
Pubblicizzare gli articoli di una rivista sull'altra in modo da suscitare interesse.
Da valutare il tutto ovviamente.
Penso che il risultato sia che chi legge la rivista per il pubblico leggerà anche quella per esperti e viceversa.

Intanto grazie per tutto l'eccelente finora fatto.

Da un affezionato

L'idea dello sdoppiamento ci frulla in testa da un po'. Abbiamo diversi responsabili IT di aziende che ci scrivono per manifestare il loro apprezzamento (e chiederci una veste più sobria). Però... Già c'è un però. In tempi di crisi, come questi, qualsiasi operazione editoriale nuova rappresenta un grosso rischio. Bisogna prima fare dei test. Accertarsi che l'idea possa funzionare. Per questo motivo abbiamo inserito la sezione Security Lab. E' il nostro laboratorio di sicurezza in cui trattiamo temi che interesseranno sicuramente tutti i lettori ma che sono mirati proprio ad un target molto professionale. Vediamo come va. In base la gradimento manifestato forse potremo valutare l'ipotesi di creare una costola di Hacker Journal che sia indirizzata proprio ad un target specializzato.

IL SUPERFLUO INDISPENSABILE

Volevo farvi notare che avete fatto dei Grandi Progressi nella rivista, ho particolarmente apprezzato l'eliminazione di molte cose superflue, la grafica migliorata e l'aggiunta di più articoli sulla sicurezza e sulla programmazione.
Il massimo sarebbe anche eliminare del tutto o quasi le immagini di teschi o cose varie, perchè alla fine non servono a nulla, per quanto riguarda il colore delle pagine per differenziare i diversi temi è OK.
Qualcosa di più mirato ogni tanto su Mac e Linux (sicurezza, programmazione) non guasterebbe, restando sempre in tema mi piacerebbe se fosse pubblicato anche un corso su Python (linguaggio a dir poco Stupendo) sui protocolli di rete, soprattutto Telnet e Ssh e un'accennata alla programmazione shell Bin/Bash. Fate quello che potete... ;-)
Oltre gli argomenti di informatica sarebbe bello trattare altri temi, ad esempio ricordo i primi numeri che compravo in cui leggevo il modo per modificare una radio facendola diventare uno scanner, tubi di pringles fatti diventare antenne Wireless.

Continuate così, state andando alla grande!

Oddio, proprio alla grande magari no, visti i risultati di vendita. Scherzi a parte la tua mail ci dà lo spunto per tornare su alcuni temi. Il primo è la grafica. Personalmente non pensiamo che i cambiamenti grafici siano cosi importanti, però visto che molti lettori ci hanno chiesto di ridurre/abbandonare parte della grafica stile Street Arts presente fin dai primi numeri, in particolare i tanti teschietti, rispondiamo volentieri a questo input inaugurando, in questo numero 205, una veste grafica più pulita. Per quanto riguarda l'apertura a Mac e Linux stiamo dedicando un po' di spazio e in questo numero trovi un ottimo articolo per Mac/Unix e almeno due dedicati a piattaforma Linux. Infine il corso di Python: è già in produzione, aspettiamo di finire il corso in C e di capire quanto spazio, a numero, possiamo dedicargli, però è certo che si farà.

CONTRIBUTO IN C

Salve, mi chiamo Carmine De Fusco e sono una accanito lettore della vostra rivista mensile "HackerJournal" anche se la seguo da poco ho notato come è sempre ben piena di contenuti grazie ai quali anche chi non è un esperto di informatica può leggerla senza trovarsi in difficoltà in quanto rendete un argomento difficile comprensibile ad una vasta gamma di utenti.

Comunque vi ho contattato per dirvi che mi piacerebbe caricare sul vostro portale un programma fatto in C che crypta i file e se vi avrebbe fatto piacere scrivere un articolo dove descrivevo l'algoritmo utilizzato per il criptaggio. L'algoritmo è molto molto semplice, sotto non c'è niente di complesso detto in poche parole il programma prende in input un qualsiasi file e in base alla password che inserisce l'utente viene criptato il file byte per byte discorso analogo per il criptaggio comunque vi invio in allegato il programmino in C , vi ripeto non è niente come algoritmo di cryptaggio ma mi sembra essere un buon esempio per chi si affaccia per la prima volta alla programmazione e vuol vedere qualcosa di concreto fatto in C senza soffermarsi ad un approccio solo teorico ma anche pratico :).

Ti ringraziamo per il contributo. Mettiamo il tuo programma nella sezione download del nostro sito (www.hackerjournal.it). Vediamo cosa ne pensano i lettori.

di Mantas
redazione@hackerjournal.it

SCAMBIARE I CONTENUTI CON PLONE E RSS

INTERNET

PLONE È STATO CREATO PER SEMPLIFICARE LA CREAZIONI DI PORTALI WEB, I RICH SITE SUMMARY PER SCAMBIARSI AGEVOLMENTE INFORMAZIONI TRA I SITI. DIAMO UNO SGUARDO AD UN CASO REALE.

Plone sta diventando una delle più diffuse tecnologie per la crezione di siti web ad alto contenuto dinamico ed elevata interazione con l'utente. In molte istanze di portali si rende necessario disporre di un sistema atto a reperire informazioni da fonti remote; un esempio è rappresentato da un gruppo di siti che condividono news.

In uno scenario del genere risulta di vitale importanza disporre di uno standard per lo scambio di informazioni. Tale standard, implementabile anche in Plone, è rappresentato da RSS.

La sua genesi è abbastanza sofferta: il protocollo RSS nasce nel 1999, quando Netscape rilascia la versione 0.90. Sono gli anni in cui Netscape punta molto sulla personalizzazione dei portali web.

Inizialmente il protocollo RSS è utilizzato prevalentemente come mezzo per l'implementazione di portali personalizzati da liste di link e news, che l'utente può aggiungere alla propria area privata. Dopo il rilascio della versione 0.91 Netscape abbandona il progetto RSS, rilevato, in seguito, da Dave Winer che l'avrebbe utilizzato come base dei sistemi di content management di Userland (www.userland.com). Contemporaneamente un altro gruppo di sviluppatori comincia a lavorare alle specifiche RSS, rilasciando la versione 1.0 del protocollo: è in questo momento che iniziano a manifestarsi i sintomi della rivalità. Winer, irritato dal rilascio della versione 1.0, inizia una serie di rilasci del protocollo RSS, che si concludono con la versione 2.0.

La situazione attuale, quindi, è la seguente: esistono due formati concorrenti che svolgono la stessa funzione. Infatti, le due specifiche hanno gli stessi elementi di base, ma una diversa filosofia di fondo. RSS 2.0 punta alla semplicità, RSS 1.0 focalizza l'attenzione sulla ricchezza semantica e all'estendibilità con moduli esterni.

SIGNIFICATO DI RSS

L'acronimo RSS, nell'accezione originaria, sta per Rich Site Summary, richiamando nel nome lo scopo per cui nasce: la descrizione dei contenuti dei portali sviluppati da Netscape. RSS significa anche RDF Site Summary, che nel nome richiama l'adozione dello standard RDF rilasciato dal W3C per la descrizione delle metainformazioni contenute, appunto, in un documento RSS.

Personalmente preferisco la seconda accezione, che racchiude intrinsecamente la natura del formato RSS, ossia la condivisione di contenuti mediante l'utilizzo dei metadati strutturati, che permettono la sindicazione di risorse web.

Le principali differenze tra i vari formati rilasciati sono riportati nella tabella seguente.

Versione RSS	Proprietario	Caratteristiche
0.90	Netscape	Struttura del documento complessa, reso obsoleto dalla versione 0.91
0.91	Userland	Ufficialmente rimpiazzato dalla versione 2.0 contiene le funzioni di base per la sindicazione dei contenuti
0.92, 0.93, 0.94	Userland	Descrizione dei metadati arricchita
1.0	RSS-DEV Working Group	Basato sulle specfiche RDF del W3C, ha una struttura che permette l'estensione del campo dei nomi di metadati con moduli aggiuntivi, non controllato da un singolo venditore
2.0	Userland	Estendibile con moduli per la sindicazione, offre funzionalità avanzate rispetto alle versioni che lo precedono, controllato da Userland che ne decide gli sviluppi.

LE PRINCIPALI DIFFERENZE TRA LE VARIE VERSIONI

Immaginiamo di voler scrivere un'applicazione in grado di leggere dai canali RSS, in modo da poter pubblicare sul proprio portale i titoli delle notizie offerte dai singoli canali. La domanda da porsi è la seguente: a che cosa assomiglia un documento RSS? La risposta dipende dalla versione di RSS utilizzata. Se, ad esempio, la fonte RSS è codifcata nel formato 0.91, si ottiene un documento del genere:

```
<rss version="0.91">
  <channel>
    <title>XML.com</title>
    <link>http://www.xml.com/</link>
    <description>XML.com features a rich mix of information and services for the XML community.</description>
    <language>en-us</language>
    <item>
      <title>Normalizing XML, Part 2</title>
      <link>http://www.xml.com/pub/a/2009/12/04/normalizing.html</link>
      <description>In this second and final look at applying relational normalization techniques to W3C XML Schema data modeling, Will Provost discusses when not to normalize, the scope of uniqueness and the fourth and fifth normal forms.</description>
    </item>
    <item>
      <title>The .NET Schema Object Model</title>
      <link>http://www.xml.com/pub/a/2009/12/04/som.html</link>
      <description>Priya Lakshminarayanan describes in detail the use of the .NET Schema Object Model for programmatic manipulation of W3C XML Schemas.</description>
    </item>
    <item>
      <title>SVG's Past and Promising Future</title>
      <link>http://www.xml.com/pub/a/2009/12/04/svg.html</link>
      <description>In this month's SVG column, Antoine Quint looks back at SVG's journey through 2008 and looks forward to 2009.</description>
    </item>
  </channel>
</rss>
```

Sembra semplice da leggere, giusto?
Un documento RSS è composto da un tag canale (channel) che contiene un tag titolo (title), link, descrizione (description), lingua (language opzionale) e un tag item che, al proprio interno, contiene di nuovo un titolo, un link e una descrizione.
Descriviamo, adesso, un formato RSS di tipo 1.0

```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns="http://purl.org/rss/1.0/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
>
  <channel
rdf:about="http://www.xml.
```

di Mantas
redazione@hackerjournal.it

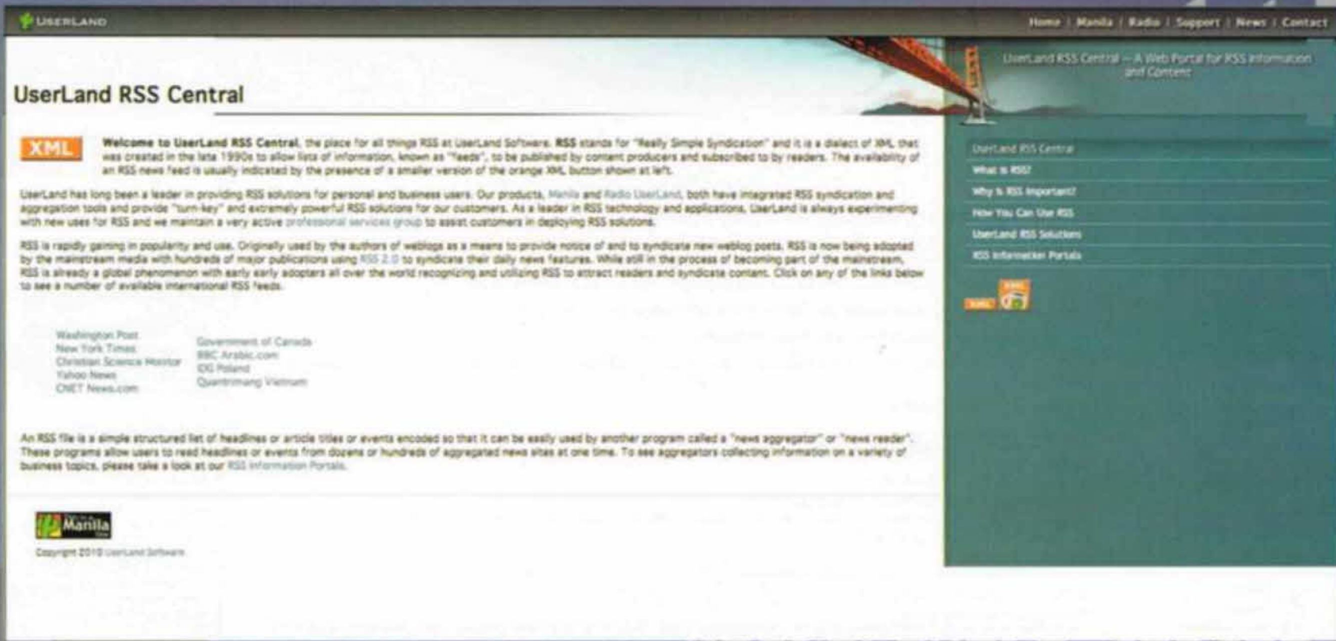
```
com/cs/xml/query/q/19">
    <title>XML.com</title>
    <link>http://www.xml.
com/</link>
    <description>XML.com fea-
tures a rich mix of informa-
tion and services for the XML
community.</description>
    <language>en-us</langua-
ge>
    <items>
      <rdf:Seq>
        <rdf:li
rdf:resource="http://www.xml.
com/pub/a/2009/12/04/normali-
zing.html"/>
        <rdf:li
rdf:resource="http://www.xml.
com/pub/a/2009/12/04/som.
html"/>
        <rdf:li
rdf:resource="http://www.xml.
com/pub/a/2009/12/04/svg.
html"/>
      </rdf:Seq>
    </items>
  </channel>
  <item rdf:about="http://
www.xml.com/pub/a/2009/12/04/
normalizing.html">
    <title>Normalizing XML,
Part 2</title>
    <link>http://www.xml.com/
pub/a/2009/12/04/normalizing.
html</link>
    <description>In this se-
cond and final look at ap-
plying relational normaliza-
tion techniques to W3C XML
Schema data modeling, Will
Provost discusses when not
to normalize, the scope of
uniqueness and the fourth and
fifth normal forms.</descrip-
tion>
    <dc:creator>Will Pro-
vost</dc:creator>
    <dc:date>2009-12-04</
dc:date>
  </item>
  <item rdf:about="http://
www.xml.com/pub/a/2009/12/04/
som.html">
    <title>The .NET Schema
Object Model</title>
    <link>http://www.xml.com/
pub/a/2009/12/04/som.html</
link>
    <description>Priya La-
kshminarayanan describes in
detail the use of the .NET
Schema Object Model for pro-
grammatic manipulation of W3C
XML Schemas.</description>
    <dc:creator>Priya La-
kshminarayanan</dc:creator>
    <dc:date>2009-12-04</
dc:date>
  </item>
  <item rdf:about="http://
www.xml.com/pub/a/2009/12/04/
svg.html">
    <title>SVG's Past and
Promising Future</title>
    <link>http://www.xml.com/
pub/a/2009/12/04/svg.html</
link>
    <description>In this
month's SVG column, Antoi-
ne Quint looks back at SVG's
journey through 2008 and loo-
ks forward to 2009.</descrip-
tion>
    <dc:creator>Antoine
Quint</dc:creator>
    <dc:date>2009-12-04</
dc:date>
  </item>
</rdf:RDF>
```

Questa versione è leggermente più complicata da comprendere.
Per chi conosce la sintassi RDF lo sforzo è quasi nullo: infatti nella versione 1.0 di RSS si richiama lo stile adottato nell' RDF; le principali differenze rispetto alla versione 0.91 sono le seguenti:

- la radice del documento cambia da rss a rdf:RDF;
- l'introduzione dei namespaces che permettono di stabilire l'ambito dei tag utilizzati nel documento;
- l'introduzione dei campi dublin core dc:date e dc:creator;
- la diversa struttura del documento RSS: cambia il tag channel che contiene un rdf:Seq ed i tag item vengono scorporati dal nodo channel.

Consideriamo, infine, lo stesso documento presentato precedentemente, codificato nella versione 2.0 del protocollo RSS.

```
<rss version="2.0"
xmlns:dc="http://purl.org/
dc/elements/1.1/">
  <channel>
    <title>XML.com</title>
    <link>http://www.xml.
com/</link>
    <description>XML.com
features a rich mix of in-
formation and services for
the XML community.</de-
scription>
    <language>en-us</lan-
guage>
    <item>
      <title>Normalizing
XML, Part 2</title>
      <link>http://www.xml.
com/pub/a/2009/12/04/norma-
lizing.html</link>
      <description>In this
second and final look at
applying relational nor-
malization techniques to
W3C XML Schema data mode-
ling, Will Provost discus-
ses when not to normalize,
the scope of uniqueness and
the fourth and fifth normal
forms.</description>
      <dc:creator>Will Pro-
vost</dc:creator>
      <dc:date>2009-12-04</
dc:date>
    </item>
    <item>
      <title>The .NET Sche-
ma Object Model</title>
      <link>http://www.xml.
com/pub/a/2009/12/04/som.
html</link>
      <description>Priya
Lakshminarayanan describes
in detail the use of the
.NET Schema Object Model
for programmatic manipula-
tion of W3C XML Schemas.</
description>
      <dc:creator>Priya La-
kshminarayanan</dc:creator>
      <dc:date>2009-12-04</
dc:date>
    </item>
    <item>
      <title>SVG's Past and
Promising Future</title>
      <link>http://www.xml.
```




```
com/pub/a/2009/12/04/svg.
html</link>
      <description>In this
month's SVG column, Antoine
Quint looks back at SVG's
journey through 2008 and
looks forward to 2009.</de-
scription>
      <dc:creator>Antoine
Quint</dc:creator>
      <dc:date>2002-12-04</
dc:date>
    </item>
  </channel>
</rss>
```

Come si può notare, anche la versione 2.0 usa i namespace, ma la struttura non rispetta i vincoli RDF. I tag item sono, come nella versione 0.91, inseriti all'interno del tag channel; inoltre restano i due tag dc:date e dc:creator presi dall'insieme dei campi dublin core.

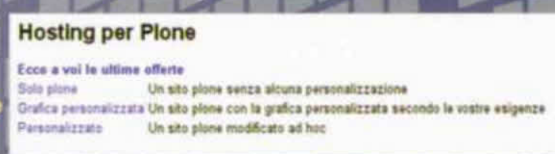
PERCHÉ RSS?

Le fonti RSS sono in pratica dei file che offrono dei contenuti ed alcuni metadati su di essi. Possono essere derivati da pagine HTML oppure creati appositamente. La caratteristica che li differenzia dagli altri contenuti web è che non sono organizzati da un punto di vista grafico, ma semantico. Con un esempio tutto ciò sarà più chiaro. Partiamo da un pezzo di HTML:

```
<table>
    <tr><td
colspan="4"><h1>Mio Sito</
h1></td></tr>
    <tr><td colspan="4"><A
href="http://www.miosito.
it"><b>Ecco a voi le ultime
offerte</b></A></td></tr>
    <tr><td><A
href="http://www.miosito.
it/soloplone">Solo plone</
A></td><td>Un sito plone
senza alcuna personalizza-
zione</td></tr>
    <tr><td><A
href="http://www.miosito.
it/mygraphic">Grafica per-
sonalizzata</A></td><td>Un
sito plone con la grafica
personalizzata secondo le
vostre esigenze</td></tr>
    <tr><td><A
href="http://
www.miosito.it/
myplone">Personalizzato</
A></td><td>Un sito plone
modificato ad hoc</td></tr>
</table>
```

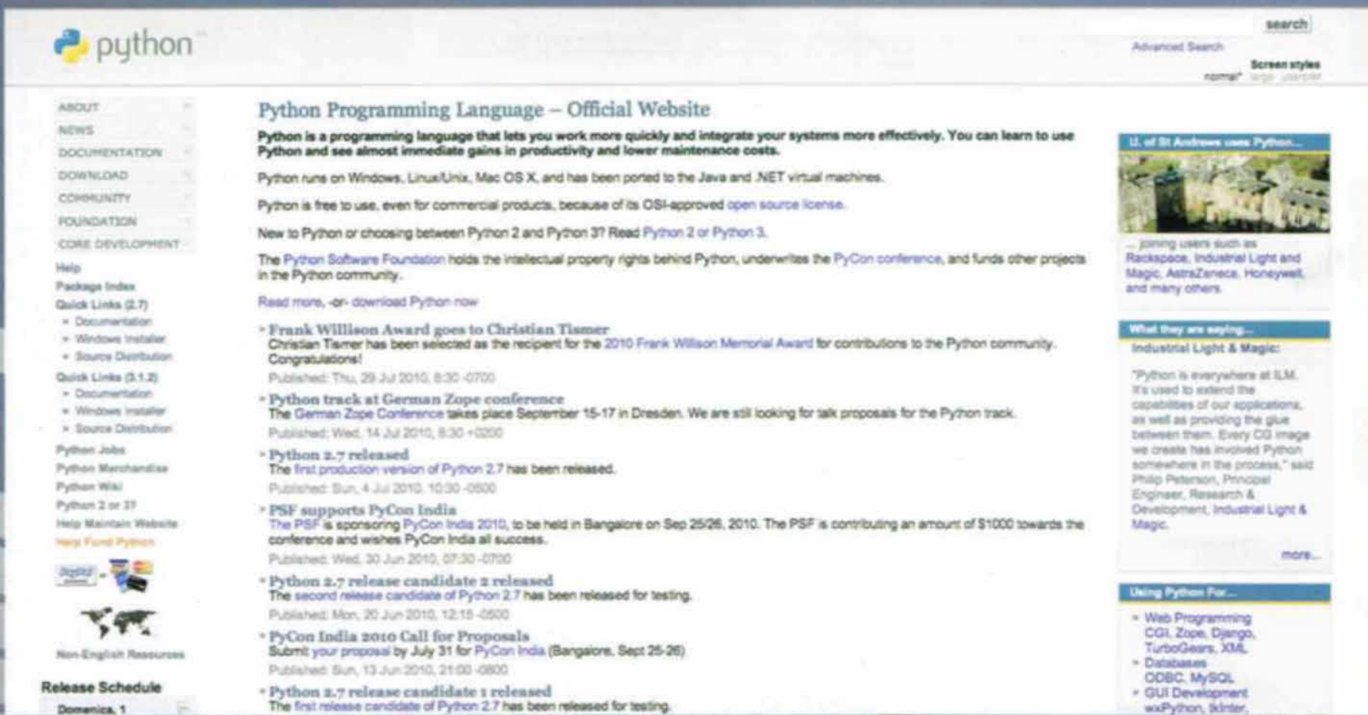
Possiamo vedere cosa generano queste poche righe nella figura riportata di seguito.

Il risultato è soddisfacente dal punto di vista grafico, ma complesso da riutilizzare come informazione. Proprio il codice è strutturato per organizzare visivamente il contenuto. Vediamolo trasformato in un semplice RSS:




```
<?xml version="1.0"?>
<rss version="0.91">
<channel>
      <title>Mio Sito</tit-
le>
<link>ttp://www.miosito.
it</link>
<description>Ecco a voi le
ultime offerte.</descrip-
tion>
<item>
      <title>Solo plone</
title>
      <link>http://www.mio-
sito.it/soloplone</link>
      <description>Un sito
plone senza alcuna persona-
lizzazione.</description>
      </item>
      <item>
      <title>Grafica perso-
```

di Mantas
redazione@hackerjournal.it




```
nalizzata</title>
      <link>http://www.mio-
sito.it/mygraphic</link>
<description>Un sito plone
con la grafica personalizza-
ta secondo le vostre esi-
genze.</description>
      </item>
      <item>

<title>Personalizzato</tit-
le>
      <link>http://www.mio-
sito.it/myplone</link>
      <description>Un sito
plone modificato ad hoc.</
description>
      </item>
</channel>
</rss>
```

Già leggendo il codice è possibile notare come l'attenzione sia posta al valore semantico dei vari elementi e cioè al loro significato. Tutto ciò senza porre alcuna attenzione a come essi verranno poi rappresentati.
Ci sarebbero ancora parecchie cose da dire su quest'argomento, soprattutto riguardo alle differenze tra le varie versioni, ma il nostro obiettivo è di vedere come sia possibile sfruttare questa tecnologia con Plone.

Effettuare ricerche su più siti Plone contemporaneamente

EFFETTUARE RICERCHE SU PIÙ SITI CON PLONE

Tra le funzionalità di Plone è presente, nel motore di ricerca interno, la generazione dinamica di un file RSS contenente l'elenco dei contenuti ricercati.Quindi è possibile interrogare un sito sulla presenza di documenti interessanti senza bisogno di navigarci sopra. Questa funzionalità è sfruttata dal prodotto PloneRSSSearch che potete scaricare qui: http://ingeniweb.sourceforge.net/Products/PloneRSSSearch/ .
Questo prodotto permette agli utenti del vostro sito di propagare automaticamente le loro ricerche su altri siti Plone. Un servizio che può essere molto utile per far risparmiare tempo e banda poiché i dati che si muovono sono solo quelli essenziali e il lavoro è svolto dal server Zope e non dai client degli utenti.
Dopo averlo installato normalmente mediante la configurazione di Plone, entrate nella Zope Management Interface (ZMI) e all'interno del vostro sito troverete un oggetto chiamato portal_rsssearch. Quest'ultimo ha due proprietà, la prima si chiama searchable_sites e al suo interno potrete scrivere gli indirizzi dei siti sui quali volete avvenga la ricerca. Un indirizzo per ogni riga.
Immaginiamo che voi dobbiate gestire il sito di una facoltà e quelli di tutti i corsi di laurea che ad essa afferiscono. In questi casi le informazioni sono spesso disperse tra i vari siti e gli utenti devo visitarne un bel numero prima di arrivare su quello giusto. Se volete evitare ai vostri utenti questa inutile complicazione basta che istalliate

PloneRSSSearch su ogni Plone configurato in modo che la ricerca avvenga sui siti correlati.
Questo servizio è disponibile solo per gli utenti registrati. Se fosse disponibile all'utente anonimo, essendo la ricerca in carico al server, qualche malintenzionato potrebbe sfruttarla per sovraccaricare la macchina che ospita il sito.

Ma, come sapete, l'accesso ai contenuti di un sito Plone è sottoposto ad una politica di sicurezza basata sui permessi che i singoli utenti hanno. Questo significa che una ricerca potrebbe non mostrare documenti a cui la persona avrebbe invece accesso. Per ovviare a questo problema ci viene incontro la seconda proprietà dell'oggetto portal_rsssearch che sia chiama _addCookie. Questa è un flag che se attivato fa sì che, con la ricerca su gli altri siti, avvenga anche l'autenticazione e cioè vengano riportati tutti i contenuti che l'utente avrebbe trovato cercando da solo. Ovviamente questa operazione funziona se lo username e la password sono la stessa. Fate attenzione ad utilizzare questa funzionalità solo se vi siete autenticati utilizzando i cookie, cioè come si fa normalmente con Plone, e non quella HTTP che viene tradizionalmente usata per la ZMI.

NON C'È SOLO PLONE!

I siti che si occupano di informazioni sono parecchi e sovente distribuiscono i loro contenuti in formato RSS, ma non è detto che siano basati su Plone. Ma questo non è un problema poiché basandoci su di un formato comune possiamo comodamente scambiarci le news. In particolare a noi interessa come mostrare quelle presenti altrove sul nostro sito Plone. Per fare ciò esistono diversi prodotti, quello che impiegheremo in questo articolo è CMFSin che ha come grande vantaggio la semplicità. L'obiettivo di questo oggetto è quello di raccogliere e organizzare delle sorgenti RSS, di mostrarne un riassunto in appositi slot laterali, simili a quelli delle normali news Plone, e di visualizzarli completamente nel corpo della pagina qualora l'utente lo richieda. Anche per l'installazione di questo prodotto è sufficiente scaricarlo all'indirizzo http://sourceforge.net/projects/collective e scompattarlo nella cartella Products della nostra istanza di Zope. Dopo aver riavviato il server ed averlo installato nella configurazione di plone all'interno della ZMI del sito Plone troverete un nuovo oggetto chiamato sin_tool. All'interno di questo oggetto, selezionando la linguetta Config è possibile definire i siti da cui estrarre le informazioni, la sintassi è questa:

```
[channels]
zopenews=http://zope.org/
news.rss
python=http://www.python.
org/pypi?:action=rss
```

e cioè assegnamo un nome ad ogni sorgente che vogliamo utilizzare. Sempre nella stessa casella dopo la sezione channel abbiamo quella maps che definisce come le nostre sorgenti saranno combinate tra loro:

```
[maps]
solo_zope=zopenews
solo_python=python
insieme=python, zopenews
```

A questo punto siete pronti per dire a Plone di mostrare le vostre fonti RSS come slot, per fare ciò è sufficiente aggiungere nelle proprietà left_slots o right_slots del vostro sito (o della cartella in cui volete che si vedano) un riferimento alla maps che volete utilizzare come se fosse una macro:

```
here/sin_tool/macros/python
here/sin_tool/macros/zope-
news
here/sin_tool/macros/insie-
me
```

Ora il vostro sito Plone è configurato per mostrare le sorgenti RSS che voi avete scelto.
Per configurazioni più raffinate aggiungo che nella sezione channel è possibile impostare il tempo di refresh per ognuna delle fonti utilizzate. Per fare ciò è sufficiente inserire prima dell'URL (separandolo con un :) la cadenza con cui aggiornare nella forma numero e unità di misura. Quest'ultima può essere sceltra tra ora (h), settimana (w), mese (m) e anno (y). Per esempio il primo canale viene aggiornato ogni 4 giorni e il secondo una volta alla settimana:

```
[channels]
zopenews=4d:http://zope.
org/news.rss
python=1w:http://www.py-
thon.org/pypi?:action=rss
```

Per le maps è anche possibile impostare la politica con cui verranno miscelate le due sorgenti. Nell'attuale versione sono presenti solo le modalità simple (che non fa nulla se non lasciare il naturale ordinamento temporale) e random (che mischia casualmente le news), ma è semplice svilupparne altre a seconda delle proprie esigenze.

```
[maps]
insieme=random:python, zo-
penews
```

Come ultimo punto aggiungo che le macro generate da sin_tool possono anche essere usate nelle proprie pagine ZPT, come ogni altra macro.

CONCLUSIONI

Le fonti RSS sono un efficace strumento per scambiare contenuti tra piattaforme differenti. Con Plone è particolarmente semplice sfruttarle grazie ai tanti prodotti che ne facilitano l'uso. Noi ne abbiamo esaminati solo due, ma ne esistono anche altri, ognuno con una particolare finalità. Anche nel caso non trovaste nulla di adatto alle vostre esigenze potreste sempre scrivervelo grazie ai funzionali e ben documentati moduli di python per la filtrazione delle sorgenti RSS.